Prof. Dr. Bettina Weisser
University of Muenster
Chair of German and International Criminal Law
Bispinghof 24/25
Germany - 48143 Muenster

Cyber Crime – The Information Society and Related Crimes

Section 2 – Special Part

National Report on Germany*

(A) Scope of questionnaire

The questions in this Section generally deal with "cyber crime". This term is understood to cover criminal conduct that affects interests associated with the use of information and communication technology (ICT), such us the proper functioning of computer systems and the internet, the privacy and integrity of data stored or transferred in or through ICT, or the virtual identity of internet users. The common denominator and characteristic feature of all cyber crime offences and cyber crime investigation can be found in their relation to computer systems, computer networks and computer data on the one hand and to cyber systems, cyber networks and cyber data on the other hand. Cyber crime covers offenses concerning traditional computer as well as cloud cyber space and cyber databases.

(B) Legislative Practices and Legal Concepts

(1) How are criminal laws related to cyber-crime codified in your country? Are they contained in a unified title or code or are they to be found in various codes or titles (Please, provide appropriate citations).

In Germany a special code of cyber crime does not exist. Many computer offences are stipulated in the Penal Code (hereinafter „PC"), yet there is no systematic approach. Computer related crimes are also stipulated in various other codes and special laws.

As for specific computer offences in the PC there are for example data espionage, sec. 202a, interception of data, sec. 202b, and acts preparatory to data espionage and interception of data, sec. 202c. Most of the "cyber crimes" are not dedicated specifically to computer offences but penalise a certain criminal behaviour and thereby encompass its commission by use of computer systems as well (for example sec. 91 „Encouraging the commission of a serious violent offence endangering the state", or sec. 111 „Public incitement to crime").

Computer-related crimes stipulated in the PC:

- Penal Code:
  - sec. 86 Dissemination of propaganda material of unconstitutional organisations
  - sec. 86a Using symbols of unconstitutional organisations

* Important notice: this text is the last original version of the national report sent by the author. The Review has not assured any editorial revision of it.

    - sec. 91 Encouraging the commission of a serious violent offence endangering the state
    - sec. 111 Public incitement to crime
    - sec. 130 Incitement to hatred
    - sec. 130a Attempting to cause the commission of offences by means of publication
    - sec. 131 Dissemination of depictions of violence
    - sec. 176 Child abuse
    - sec. 184 Distribution of pornography
    - sec. 184a Distribution of pornography depicting violence or sodomy
    - sec. 184b Distribution, acquisition and possession of child pornography
    - sec. 184c Distribution, acquisition and possession of juvenile pornography
    - sec. 184d Distribution of pornographic performances by broadcasting, media services or telecommunications services
    - sec. 202a Data espionage
    - sec. 202b Interception of data
    - sec. 202c Acts preparatory to data espionage and phishing
    - sec. 203 Violation of private secrets
    - sec. 206 Violation of the postal and communication secret
    - sec. 238 Stalking
    - sec. 263a Computer fraud
    - sec. 265a Obtaining services by deception
    - sec. 269 Forgery of data intended to provide proof
    - sec. 270 Meaning of deception in the context of data processing
    - sec. 274 Suppression of documents; changing a border mark
    - sec. 284 Organising unlawful gaming
    - sec. 285 Participation in unlawful gaming
    - sec. 287 Organising an unlawful lottery etc
    - sec. 303a Data tampering
    - sec. 303b Computer sabotage
    - sec. 317 Disruption of telecommunications facilities
    - sec. 353b Breach of official secrets and special duties of confidentiality

Apart from the offences mentioned in the PC a few special codes contain regulations on specific computer offences regarding the general scope of the special code. A few examples only:

- Federal Data Protection Act (BDSG)
    - sec. 43 Administrative offences
    - sec. 44 Criminal offences
- Copyright Act (UrhG)
    - sec. 106 Unauthorized exploitation of copyrighted works
    - sec. 108 Infringement of neighbouring rights
    - sec. 108a Unlawful exploitation on a commercial basis
- German Art Copyright Act (KUG)
    - sec. 33 Criminal offences

- Protection of Young Persons Act (JuSchG)
  - sec. 27 Criminal offences
  - sec. 28 Administrative offences
- Telecommunications Act (TKG)
  - sec. 148 Criminal offences
  - sec. 149 Administrative offences
- Act against Unfair Competition (UWG)
  - § 17 Disclosure of trade and industrial secrets

(2) What is the impact of judicial decisions on the formulation of criminal law related to cyber-crimes?

There is only limited impact of judicial decisions on the German legislature. Only very few judgments have led to amendments of the law on cybercrime:

In the year 2007 **sec. 303b PC** was amended and a new regulation came into force. Sec. 303b subsec. 1 no. 2[1] rules that, unless it is not authorized, the entering as well as the transmitting of data into computer systems is a criminal offence. The regulation is meant to cover "denial-of-service-attacks" in particular. The new regulations were prompted by a judicial decision of the Higher Regional Court of Frankfurt aM (22.5.2006 -1 Ss 319/05).

In that case, the perpetrator had initiated an "online-demonstration" consisting of a denial-of-service-attack against the website of the German Lufthansa. He wanted to protest against the company's support of the German deportation practice by flying foreign illegal residents out of the country. The court stated that the conduct of organizing an "online-demonstration" cannot be seen as a criminal offence under the German Penal Code as the temporary suppression of access or of data (by denial-of-service-attacks) was not punishable. For this reason the German legislator stipulated it as an offence to "enter or transmit data with the intention of causing damage to another". The perpetrator in the case clearly had had this intention.

[1] **Sec. 303b PC Computer sabotage**
(1) Whosoever interferes with data processing operations which are of substantial importance to another by 1. committing an offence under section303a(1); or 2. entering or transmitting data (section 202a(2)) with the intention of causing damage to another; or 3. destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier, shall be liable to imprisonment not exceeding three years or a fine.
(2) If the data processing operation is of substantial importance for another's business, enterprise or a public authority, the penalty shall be imprisonment not exceeding five years or a fine.
(3) The attempt shall be punishable.
(4) In especially serious cases under subsection (2) above the penalty shall be imprisonment from six months to ten years. An especially serious case typically occurs if the offender 1. causes major financial loss, 2. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of computer sabotage, or 3. through the offence jeopardises the population's supply with vital goods or services or the national security of the Federal Republic of Germany.
(5) Section 202c shall apply mutatis mutandis to acts preparatory to an offence under subsection (1) above.
Sec. 303a PC Data tampering
(1) Whosoever unlawfully deletes, suppresses, renders unusable or alters data (section 202a (2)) shall be liable to imprisonment not exceeding two years or a fine.
(2) The attempt shall be punishable.

What is more, the legislator established it as an aggravating factor if the attack targeted at a data processing system of substantial importance for another's "business, enterprise or public authority"[2]. It is important to understand that this new regulation criminalizes a behaviour which would be perfectly legal – if it were not committed simultaneously by a great number of people acting with a shared intent to cause damage to the host of the addressed website.

The **Code of Criminal Procedure** will be amended in the near future as well: German opponents of the law on data retention measures had filed a claim to the German Federal Constitutional Court against the new laws on data retention in Germany. They were based upon a EU Directive. The Constitutional Court declared the regulations as unconstitutional and therefore void[3]. Ironically one of the former successful appellants against the laws is today Germany's Federal Secretary of Justice and she has to support the opposite position now as Germany is obliged to adapt the national law to the EU Directive guidelines. So the German legislator is bound to establish new rules on data retention – yet the legislative organs seem to be trapped in a serious deadlock concerning this area of the law. It is to be expected that there will be only limited progress concerning this matter prior to the elections to parliament in autumn 2013.

(3) To catch up with changing needs and circumstances and to attain new objectives, some laws, instead of simply modifying the parts of the law that need to be changed, present the required amendments into a consolidated text together with all past amendments. This technique is called recasting. Is that how cyber-crime laws are updated and adapted to changed realities in your country? Please provide appropriate references and citations.

As has been mentioned before, there does not exist a specific unified code on cyber crime in Germany. In some fields of the law the legislator aims at amending existing regulations to adapt the law to new developments in computer technology[4]. Still no plans exist on establishing new rules in a consistent new statute specificially dedicated to cyber crime[5].

Particular amendments of the current law concerning cyber crime follow the basic rules on lawmaking in Germany[6]. This means that existing laws are amended or new regulations are incorporated in existing codes. The recent amendments of sec. 202a-202c[7] and sec. 303a-303c

[2] Sec. 303b PC II, see footnote 1.
[3] BVerfGE 125, 260 ff.
[4] *Sieber,* Report on Criminal Offences and Prosecution in Cyberspace, „Straftaten und Strafverfolgung im Internet, 69. Deutschen Juristentag 2012, C 84 ff. u. C 154 f.; Resolution of the 69. German Juristentag, Section of Criminal Law, II. 1., p. 9: http://www.djt.de/fileadmin/downloads/69/120921_djt_69_beschluesse_web_rz.pdf.
[5] *Hilgendorf,* JZ 2012, 825, 832; vgl. *Kurz,* in Thesen der Gutachter und Referenten zum 69. DJT, S. 36, http://www.djt.de/fileadmin/downloads/69/120809_djt_69_thesen_web.pdf.
[6] For an overview see the official guidelines of the Ministry of Justice „Handbuch der Rechtsförmlichkeit": http://hdr.bmj.de.
[7] **Section 202a PC: Data espionage**
(1) Whosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorised access, if he has circumvented the protection, shall be liable to imprisonment not exceeding three years or a fine.
(2) Within the meaning of subsection (1) above data shall only be those stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable.

PC[8] can be mentioned as examples. The same way new regulations on Child Pornography have been included in sec. 176, 184b, 184c, 184d - 184f PC[9] to transpose the European

---

Section 202b PC: Interception of data
Whosoever unlawfully intercepts data (section 202a(2)) not intended for him, for himself or another by technical means from a non-public data processing facility or from the electromagnetic broadcast of a data processing facility, shall be liable to imprisonment not exceeding two years or a fine, unless the offence incurs a more severe penalty under other provisions.
Section 202c PC: Acts preparatory to data espionage and phishing
(1) Whosoever prepares the commission of an offence under section 202a or section 202b by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible
1. passwords or other security codes enabling access to data (section 202a(2)), or
2. software for the purpose of the commission of such an offence, shall be liable to imprisonment not exceeding one year or a fine.
(2) Section 149(2) and (3) shall apply mutatis mutandis.
[8] See footnote 1 and:
Section 303c PC: Request to prosecute
In cases under sections 303 to 303b the offence may only be prosecuted upon request, unless the prosecuting authority considers propio motu that prosecution is required because of special public interest.
[9] **Section 176 PC: Child abuse**
(1) Whosoever engages in sexual activity with a person under fourteen years of age (child) or allows the child to engage in sexual activity with himself shall be liable to imprisonment from six months to ten years.
(2) Whosoever induces a child to engage in sexual activity with a third person or to allow third persons to engage in sexual activity with the child shall incur the same penalty.
(3) In especially serious cases the penalty shall be imprisonment of not less than one year.
(4) Whosoever 1. engages in sexual activity in the presence of a child; 2. induces the child to engage in sexual activity, unless the act is punishable under subsection (1) or subsection (2) above; 3. presents a child with written materials (section 11(3)) to induce him to engage in sexual activity with or in the presence of the offender or a third person or allow the offender or a third person to engage in sexual activity with him; or 4. presents a child with pornographic illustrations or images, audio recording media with pornographic content or pornographic speech,
shall be liable to imprisonment from three months to five years.
(5) Whosoever supplies or promises to supply a child for an offence under subsections (1) to (4) above or who agrees with another to commit such an offence shall be liable to imprisonment from three months to five years.
(6) The attempt shall be punishable; this shall not apply to offences under subsection (4) Nos 3 and 4 and subsection (5) above.
Section 184b PC: Distribution, acquisition and possession of child pornography
(1) Whosoever
1. disseminates;
2. publicly displays, presents, or otherwise makes accessible; or
3. produces, obtains, supplies, stocks, offers, announces, commends, or undertakes to import or export in order to use them or copies made from them within the meaning of Nos 1 or 2 above or facilitates such use by another pornographic written materials (section 11 (3)) related to sexual activities performed by, on or in the presence of children (section 176 (1)) (child pornography) shall be liable to imprisonment from three months to five years.
(2) Whosoever undertakes to obtain possession for another of child pornography reproducing an actual or realistic activity shall incur the same penalty.
(3) In cases under subsection (1) or subsection (2) above the penalty shall be imprisonment of six months to ten years if the offender acts on a commercial basis or as a member of a gang whose purpose is the continued commission of such offences and the child pornography reproduces an actual or realistic activity.
(4) Whosoever undertakes to obtain possession of child pornography reproducing an actual or realistic activity shall be liable to imprisonment not exceeding two years or a fine. Whosoever possesses the written materials set forth in the 1st sentence shall incur the same penalty.
(5) Subsections (2) and (4) above shall not apply to acts that exclusively serve the fulfilment of lawful official or professional duties.

Framework Decision (2004/68/JHA) of 22 December 2003 on combating the sexual exploitation of children and child pornography[10] into German Law[11].

A different approach was chosen concerning the law on unfair competition and the law on data protection. Two new statutes came into force in the years 2004 (Act Against Unfair Competition) and 1990 (Federal Data Protection Act) and repealed the pre-existing regulations. Since then only amendments have been made to those laws. Consolidated versions of the acts have been published. Yet as far as a former version is announced once again in a con-

---

(6) In cases under subsection (3) above section 73d shall apply. Objects to which an offence under subsection (2) or (4) above relates shall be subject to a depriation order. Section 74a shall apply.

Section 184c PC: Distribution, acquisition and possession of juvenile pornography

(1) Whosoever

1. disseminates;
2. publicly displays, presents, or otherwise makes accessible; or
3. produces, obtains, supplies, stocks, offers, announces, commends, or undertakes to import or export in order to use them or copies made from them within the meaning of Nos 1 or 2 above or facilitates such use by another pornographic written materials (section 11 (3)) related to sexual activities performed by, on or in the presence of persons between the ages of fourteen to eighteen years (juvenile pornography) shall be liable to imprisonment not exceeding three years or a fine.

(2) Whosoever undertakes to obtain possession for another of juvernile pornography reproducing an actual or realistic activity shall incur the same penalty.

(3) In cases under subsection (1) or subsection (2) above the penalty shall be imprisonment of three months to five years if the offender acts on a commercial basis or as a member of a gang whose purpose is the continued commission of such offences and the juvenile pornography reproduces an actual or realistic activity.

(4) Whosoever undertakes to obtain possession of child pornography reproducing an actual or realistic activity shall be liable to imprisonment not exceeding one year or a fine. The 1st sentence shall not apply to acts of persons related to juvenile pornography produced by them while under eighteen years of age and with the consent of the persons therein depicted.

(5) Section 184b (5) and (6) shall apply mutatis mutandis.

Section 184d PC: Distribution of pornographic performances by broadcasting, media services or telecommunications services

Whosoever disseminates pornographic performances via broadcast, media services, or telecommunications services shall be liable pursuant to sections 184 to 184c. In cases under section 184 (1) the 1st sentence above shall not apply to dissemination via media services or telecommunications services if it is ensured by technical or other measures that the pornographic performance is not accessible to persons under eighteen years of age.

Section 184e PC: Unlawful prostitution

Whosoever persistently contravenes a prohibition enacted by ordinance against engaging in prostitution in particular places at all or during particular times of the day, shall be liable to imprisonment not exceeding six months or a fine not exceeding one hundred and eighty daily units.

Section 184f PC: Prostitution likely to corrupt juveniles

Whosoever engages in prostitution

1. in the vicinity of a school or other locality which is intended to be visited by persons under eighteen years of age; or
2. in a house in which persons under eighteen years of age live, in a way which is likely to morally corrupt these persons, shall be liable to imprisonment not exceeding one year or a fine.

[10] European Framework Decision (2004/68/JHA) of 22 December 2003 on combating the sexual exploi-tation of children and child pornography: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:013:0044:0048:EN:PDF. The Framework Decision (2004/68/JHA) has been replaced by the Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography.

[11] Gesetz zur Umsetzung des Rahmenbeschlusses des Rates der europäischen Union zur Bekämpfung der sexuellen Ausbeutung von Kindern und Kinderpornographie vom 31.10.2008, BGBl. I 2149; 2008 Federal Law Gazette I, p. 2149.

solidated version, the announcement only has a declarative effect. The current versions of the acts can be accessed: Act Against Unfair Competition, 3 March 2010[12], Federal Data Protection Act, 1 April 2010 and 11 June 2010[13].

(C) The Specific Cybercrime Offenses

(1) Concerning mens rea, must cybercrime offenses be intentional? Do they require a specific intent?

Most of the cyber crime offences require intent (sec. 15 PC[14]). "German intent" means that the perpetrator at least must have recognized the risk and acted anyway knowing that the risk might be realized in an infringement of legally protected interests. However, some offences require more than this most lenient form of mens rea. The perpetrator either must have been sure that a violation of legally protected interests would occur or must specifically have intended a certain profit which inevitably leads to a violation of legally protected interests of others[15].

(2) Are there also negligent offenses in this field?

Most of the criminal offences concerning cyber crime require intent. Only very few offences can be committed negligently. Cyber crime offences established as adminstrative offences on the other hand criminalize intentional as well as negligent behaviour.

(3) If yes, please, provide a list of those offenses.

- sec. 317 III PC[16]
- sec. 148 II Telecommunications Act[17]

[12] 2010 Federal Law Gazette [BGBl.]) Part I p. 254. Act Against Unfair Competition: http://www.gesetze-im-internet.de/englisch_uwg/the_act_against_unfair_competition.pdf.

[13] 2003 Federal Law Gazette I, p. 66; 2009 Federal Law Gazette I, p. 2814. Federal Data Protection Act: http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile.

[14] **Section 15 PC: Intent and negligence**
Unless the law expressly provides for criminal liability based on negligence, only intentional conduct shall attract criminal liability.

[15] Computer fraud, sec. 263: intent of obtaining unlawful material benefits; sec. 44 Federal Data Protection Act: intent of enriching himself or others.

[16] **Section 317 Disruption of telecommunications facilities**
(1) Whosoever prevents or endangers the operation of a telecommunications facility which serves public purposes by destroying, damaging, removing, altering or rendering unusable an object which serves its operation, or taps electrical power intended for its operation shall be liable to imprisonment not exceeding five years or a fine.
(2) The attempt shall be punishable.
(3) Whosoever commits the offence negligently shall be liable to imprisonment not exceeding one year or a fine.

[17] **Section 148: Penal Provisions**
(1) Any person who,

- sec. 23 JMStV – JugendmedienschutzG - Staatsvertrag
- sec. 27 subsec. 3 Youth Protection Act
- Administrative offences
  - Sec. 43 BDSG[18]
  - Sec. 149 Telecommunications Act[19]
  - Sec. 16 II TMG
  - Sec. 24 JMStV
  - Sec. 28 Youth Protection Act

(a) Integrity and functionality of the IT system

1. Illegal access and interception of transmission

a. Object – system or data?

Does your criminal law establish as a criminal offense the serious hindering, without right, of the function of a computer and/or electronic system by inputting, transmitting, damaging, deleting, de-

---

1. in contravention of section 89 sentence 1 or 2, intercepts a communication or imparts to others the content of a communication or the fact of its reception; or
2. in contravention of section 90(1) sentence 1,
a) owns, or
b) manufactures, markets, imports or otherwise introduces in the area of application of this Act transmitting equipment as referred to there, is liable to a term of imprisonment not exceeding two years, or to a financial penalty.
(2) Where action in the cases of subsection (1) para 2 b) arises through negligence, the offender is liable to a term of imprisonment not exceeding one year, or to a financial penalty.

Section 89: Prohibition to Intercept, Obligation on Receiving Equipment Operators to Maintain Privacy
Interception by means of radio equipment shall be permitted only for communications intended for the radio equipment operator, radio amateurs within the meaning of the Amateur Radio Act of 23 June 1997 (Federal Law Gazette Part I page 1494), the general public or a non-defined group of persons. The content of communications other than those referred to in sentence 1 and the fact of their reception, even where reception has been unintentional, may not, even by persons not already committed to privacy under section 88, be imparted to others. Section 88(4) applies accordingly. The interception and passing on of communications by special legal authorization remain unaffected.

[18] **Section 43 Administrative offences**
(1) An administrative offence shall be deemed to have been committed by anyone who, whether intentionally or through negligence
1. in violation of Section 4d (1), also in conjunction with Section 4e second sentence, fails to notify, fails to do so within the prescribed time limit or fails to provide complete information,
…
(3) Administrative offences may be punished by a fine of up to € 50,000 in the case of subsection 1, and a fine of up to € 300,000 in the cases of subsection 2. The fines should exceed the financial benefit to the perpetrator derived from the administrative offence. If the amounts mentioned in the first sentence are not sufficient to do so, they may be increased.

[19] **Section 149 Administrative Fines Provisions**
(1) An administrative offence is deemed to have been committed by any person who, intentionally or negligently,
1. in contravention of section 4, fails to provide information, to provide it correctly, to provide it completely or to provide it in timely manner;
…
35. in contravention of section 113(1) sentence 4, fails to maintain silence. …

teriorating, altering or suppressing information or data from a computer system, software or program?

Yes, sec. 303b PC[20] (computer sabotage) criminalizes the acts referred to above. However, this provision does not imply violations of computer systems, software or programs (except for subsec. 1 no. 3, explicitly mentioning data processing equipment or data storage mediums). In fact, data processing operations of significant importance are targeted by this offence.

Referring to the offence of **computer sabotage (sec. 303b PC)**, the German PC divides the penalized actions up into 3 modes of conduct:

1. The described acts are punishable under sec. 303b, 303a PC if they have caused considerable damages of data processing equipment.

2. Sec. 303b subsec. 1 no. 1 PC implies with reference to sec. 303a PC the deleting, suppressing, disabling or altering of data. In subsec. 1 no. 2, actions of input or transmission of data are enlisted (sec. 202a subsec. 2 PC). These acts require the perpetrator's intention to cause damage to another.

3. Finally, subsec. 3 criminalizes the destroying, damaging, rendering unusable, removing or altering of a data processing system or a data carrier.

Apart from this, **sec. 317 PC**[21] penalizes the **disruption of telecommunication facilities**. The provision only refers to telecommunication systems which serve public purposes. This pre-

[20] **Section 303b Computer sabotage**
(1) Whosoever interferes with data processing operations which are of substantial importance to another by
1. committing an offence under section303a(1); or
2. entering or transmitting data (section 202a(2)) with the intention of causing damage to another; or
3. destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier,
shall be liable to imprisonment not exceeding three years or a fine.
(2) If the data processing operation is of substantial importance for another's business, enterprise or a public authority, the penalty shall be imprisonment not exceeding five years or a fine.
(3) The attempt shall be punishable.
(4) In especially serious cases under subsection (2) above the penalty shall be imprisonment from six months to ten years. An especially serious case typically occurs if the offender
1. causes major financial loss,
2. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of computer sabotage, or
3. through the offence jeopardises the population's supply with vital goods or services or the national security of the Federal Republic of Germany.
(5) Section 202c shall apply mutatis mutandis to acts preparatory to an offence under subsection (1) above.
Section 303a Data tampering
(1) Whosoever unlawfully deletes, suppresses, renders unusable or alters data (section 202a (2)) shall be liable to imprisonment not exceeding two years or a fine.

[21] **Section 317 PC: Disruption of telecommunications facilities**
(1) Whosoever prevents or endangers the operation of a telecommunications facility which serves public purposes by destroying, damaging, removing, altering or rendering unusable an object which serves its operation, or taps electrical power intended for its operation shall be liable to imprisonment not exceeding five years or a fine.

condition is met if the system is meant to serve (mainly) public interests[22]. The term "telecommunications systems" describes technical facilities or equipment capable of sending, transmitting, switching, receiving, steering or controlling electromagnetic or optical signals identifiable as messages[23]. The criminalized behaviour may consist of the destroying, damaging, removing, altering or rendering unusable an object which serves its operation, or of the tapping of electrical power intended for the administration of the telecommunication system. Concerning cybercrime the main focus lies on the alternatives of rendering unusable and of altering of a data processing system or a data carrier, i.e. these acts do not comprise the damaging of the system or carrier. An example would be a denial-of-service-attack[24].

Dedicated to the protection of financial interests is the offence of **computer fraud, sec. 263a PC** [25]. The criminalized conduct comprises four forms of damaging the financial interests of another by means of a computer. The conduct can consist of

- influencing the result of a data processing operation through incorrect configuration of a program
- the use of incorrect or incomplete data
- the unauthorized use of data or
- other unauthorized influence on the course of the processing.

The different modes of conduct are partly overlapping and cannot easily be distinguished. The goal of the legislator was to penalize all kinds of manipulation leading to financial damages. The different acts refer to the different stages of data processing operations: manipulation of data input, manipulation of the processing of data, manipulation of data output or hardware manipulation.[26]

b. Requirement of infringement of security measures?

Is it a requirement of your criminal law that the hacker conduct the hack of the computer system by using one or more software needed to defeat security measures and gain entry-level or higher level of access?

Hacking is penalized as per sec. 202a PC[27]. The provision came into force in the year 2007[28] and was meant to adapt the German Criminal Law to the regulations of the Cybercrime-

(2) The attempt shall be punishable.
(3) Whosoever commits the offence negligently shall be liable to imprisonment not exceeding one year or a fine.

[22] Schönke/Schröder, Commentary on the PC (2010)- *Sternberg-Lieben/Hecker (hereinafter: „S/S-author"),* § 317 marginal no. 3; Systematic Commentary on the PC-*Wolters (hereinafter: „SK-author"),* § 317 marginal no. 5.

[23] This definition is to be found in sec. 3 no. 23 Telecommunications Act (TKG).

[24] *Gercke/Brunst,* Praxishandbuch Internetstrafrecht, marginal no. 150.

[25] **Section 263a PC: Computer fraud**
(1) Whosoever with the intent of obtaining for himself or a third person an unlawful material benefit damages the property of another by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorised use of data or other unauthorised influence on the course of the processing shall be liable to imprisonment not exceeding five years or a fine. ...

[26] S/S-*Cramer/Perron,* § 263a marginal no. 4.

[27] **Section 202a PC Data espionage**

Convention of the Council of Europe (2001)[29] and of the European Framework Decision on attacks against information systems (2005)[30]. To restrict the ambit of the provision, the German legislator defined that only data that are specifically protected against unlawful attacks fall within the purview of sec. 202a PC[31].

Concerning industrial espionage, according to sec. 17 subsec. 2 no.1 of the Act against Unlawful Competition[32] the infringement of a security measure is not a requirement of the offence description. Still, the scope of the provision is restricted by the need to actually disclose a trade or industrial secret – mere „hacking" as such does not result in an offence under sec. 17 subsec. 2 no. 1 of the Act against Unlawful Competition[33].

2. Data and system interference

a. Object – protection of system/hardware/data?

Does your criminal law define "computer and/or electronic data"? Does this definition include programs or software or similar coding? If you have a definition, please provide it and the reference to the related paragraphs/articles of your code.

There is no legal definition of computer and/or electronic data provided in German Criminal Law, since the legislator felt that there was no need for such a definition[34].

---

(1) Whosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorised access, if he has circumvented the protection, shall be liable to imprisonment not exceeding three years or a fine.
(2) Within the meaning of subsection (1) above data shall only be those stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable.

[28] 2007 Federal Law Gazette [BGBl.]) Part I p. 1786.

[29] ETS No. 185.

[30] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:EN:PDF.

[31] This restriction is established compliant to art. 2 subsec. 2 of the Framework Decision (= art. 2 subsec. 2 of the Cybercrime-convention): „2. Each Member State may decide that the conduct referred to in paragraph 1 is incriminated only where the offence is committed by infringing a security measure."

[32] **Section 17 Act against Unlawful Competition: Disclosure of trade and industrial secrets**
(1) Whoever as the employee of a business communicates, without authorisation, a trade or industrial secret with which he was entrusted, or to which he had access, during the course of the employment relationship to another person for the purposes of competition, for personal gain, for the benefit of a third party, or with the intent of causing damage to the owner of the business shall be liable to imprisonment not exceeding three years or to a fine.
(2) Whoever for the purposes of competition, for personal gain, for the benefit of a third party, or with the intent of causing damage to the owner of the business, acquires or secures, without authorisation,
1. a trade or industrial secret
a) by using technical means;
b) by creating an embodied communication of the secret; or
c) by removing an item in which the secret is embodied; or
2. without authorisation, uses or communicates to anyone a trade secret which he acquired through one of the communications referred to in subsection (1), or through an act of his own or of a third party pursuant to number 1, or which he has otherwise acquired or secured without authorisation shall incur the same liability. …

[33] BT-Drucks. 16/3656, p. 9. Köhler/Bornkamm-*Köhler,* Commentary on the Federal Data Protection Act (hereinafter: UWG), § 17, marginal no. 30.

[34] BT-Drucks. 10/5058, p. 29.

However, sec. 202a subsec. 2 includes a restriction of the provision's ambit to data "stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable"[35]. This term is used as a reference for other provisions using the term "data" and therefore somehow serves as a legal definition. Still, apart from the restriction of data to those electronically or magnetically transmitted, the regulation does not imply a definition as to what the term data as such is supposed to mean.[36]

Scholars suggest that the term data means an electronic description of information[37]. This definition encompasses software programs since they consist of data as well.[38]

b. Act – destruction/alteration/rendering inaccessible?

i. Does your penal law penalize the unauthorized erasure, alteration, rendering inaccessible, acquiring or other similar interference with information or data from a computer or electronic system or program?

The alteration of data is punishable under sec. 303a PC[39]. As for a definition of the protected data the provision refers to sec. 202a subsec. 2 PC. The provision criminalizes the deletion, suppression, rendering unusable or altering of data. The criminalized acts cannot easily be distinguished and overlap each other. Sec. 202a subsec. 2 PC is meant to cover every act of illegal manipulation affecting the use of data.[40] Yet the wording of the provision reaches much too far – since it could be seen as an offence under sec. 303a PC if a person alters data that he or she had lawfully created or stored before. So the prevailing opinion suggests a restriction of the provision's ambit by the prerequisite that the perpetrator must have acted without authority to do so.

If data of legal relevance are affected by a manipulation, the special provision of sec. 274 PC[41] comes into play: It criminalizes the deletion, suppression, rendering unusable or altering

[35] Sec. 202a PC, see. footnote 27.
[36] S/S-*Lenckner/Eisele,* § 202a, marginal no. 2.
[37] Leipzig Commentary to the PC-*Hilgendorf* (hereinafter: „LK-author"), § 202a marginal no. 7; LK-*Wolff,* § 303a marginal no. 6; *Schulze-Heiming,* Der strafrechtliche Schutz der Computerdaten gegen die Angriffsformen der Spionage, Sabotage und des Zeitdiebstahls (1995), p. 26; NK-*Kargl,* § 303a, marginal no. 4.
[38] BT-Drucks. 10/5058, p. 29; NK-*Kargl,* § 202a, marginal no. 4; S/S-*Lenckner/Eisele,* § 202a, marginal no. 3.
[39] **Section 303a PC Data tampering**
(1) Whosoever unlawfully deletes, suppresses, renders unusable or alters data (section 202a (2)) shall be liable to imprisonment not exceeding two years or a fine.
(2) The attempt shall be punishable.
[40] BT-Drucks. 10/5058, p. 34.
[41] **Section 274 PC: Suppression of documents; changing a border mark**
(1) Whosoever
1. destroys, damages or suppresses a document or a technical record which does not belong to him or not exclusively to him with the intent of causing damage to another;
2. deletes, suppresses, renders unusable or alters legally relevant data (section 202a(2)), which are not or not exclusively at his disposal, with the intent of causing damage to another; or
3. takes away, destroys, renders unrecognisable, moves or falsely places a border stone or another sign intended as a designation of a border or water level with the intent of causing damage to another, shall be liable to imprisonment not exceeding five years or a fine.

of data that can serve as a piece of evidence in legal matters. The offence requires that the perpetrator aims at causing damage to the person who is authorized to use the data. This damage consists of the loss or of the impairment of the evidence. It is not required that the damage be a financial one.

The offence of Computer Fraud, sec. 263a PC[42] however refers to financial damages that are caused by a manipulation of computer data processing operations. This provision not only comprises the manipulation of data but the manipulation of computer programs as well[43].

ii. Does your penal law penalize the unauthorized interception of the transmission in any manner or mode of computer or electronic data and/or information?

Yes, those acts are subject to sec. 202b PC[44]. The provision penalizes the unlawful interception of data by technical means. The provision came into force in the year 2007[45] to fill in a gap, since before no offence was especially dedicated to the unauthorized interception of the transmission of data. Sec. 201 PC and sec. 148, 89 Telecommunications Act criminalized the interception of telecommunication (wiretapping), whereas sec. 202a PC[46] is restricted to specifically protected data. So sec. 202b PC aims at criminalizing every unauthorized interception of the transmission of data by technical means.[47]

3. Data Forgery

a. Object – authenticity?

Does your penal law define as a criminal offense the unauthorized input, alteration, deletion or suppression of computer or electronic data resulting in authentic data in order to protect the authenticity of the data to be used or acted upon for legal purposes? If you have a definition, please provide it along with the reference to the related paragraphs/articles of your code and/or special statutes.

---

(2) The attempt shall be punishable.

[42] **Section 263a PC: Computer fraud**

(1) Whosoever with the intent of obtaining for himself or a third person an unlawful material benefit damages the property of another by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorised use of data or other unauthorised influence on the course of the processing shall be liable to imprisonment not exceeding five years or a fine. …

[43] *Fischer* Commentary to the PC (2013) (hereinafter: "Fischer"), § 263a marginal no. 6; *Lackner/Kühl,* Commentary to the PC (hereinafter: "Lackner/Kühl"), § 263a marginal no.6.

[44] **Section 202b PC Interception of data**

Whosoever unlawfully intercepts data (section 202a(2)) not intended for him, for himself or another by technical means from a non-public data processing facility or from the electromagnetic broadcast of a data processing facility, shall be liable to imprisonment not exceeding two years or a fine, unless the offence incurs a more severe penalty under other provisions.

[45] 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG) vom 07.08.2007 (2007 Federal Law Gazette I p. 1786)

[46] Sec. 202a Data espionage, see footnote 27.

[47] BT-Drucks. 16/3656, S. 11.

The definition of a falsified document under German Criminal Law is that the person appearing as the document's author is not its true author. German Law on the forgery of documents does not protect the public's interest in the truthfulness of a document's content but only the public's interest in the author's true identity. Therefore it is not conceivable under German Criminal Law on data forgery that the unauthorized input of computer or electronic data result in authentic data. Hence, if a person who is not authorized to produce electronic data manages to do so, the produced document – if any – will most likely appear as produced by a different author. In this case the requirements of the offence of forgery of documents/data (see 3.b.) will be met.

b. Act – alteration/deletion?

Does your penal law penalize as a criminal offense the unauthorized input, alteration, deletion or suppression of computer or electronic data/information resulting in inauthentic data/information with the intent that it be considered or acted upon for legal purposes as if it were authentic? If yes, please provide the reference to the applicable paragraphs/articles of your code.

Yes, those acts are subject to sec. 269 PC[48]. The provision refers to data that are intended to provide legal proof. The offence consists of a manipulation of data that would produce a falsified document if the data were embodied in a document. An abstract definition of legally protected data does not exist. However, it can be derived indirectly from the offence description of sec. 267 PC[49]. Sec. 267 PC criminalizes the forgery of documents. The term document is defined by its functions:

1. It is meant to perpetuate a declaration/statement
2. It has to reveal the true author of the document ("guarantee function")
3. It is meant to give legal proof of the author (function of proof)

The product of a punishable data manipulation under sec. 269 PC must be an output that would amount to a falsified document in the sense of sec. 267 PC if it were embodied in a

[48] **Section 269 PC Forgery of data intended to provide proof**
(1) Whosoever for the purposes of deception in legal commerce stores or modifies data intended to provide proof in such a way that a counterfeit or falsified document would be created upon their retrieval, or uses data stored or modified in such a manner, shall be liable to imprisonment not exceeding five years or a fine.
...

[49] **Section 267 PC Forgery**
(1) Whosoever for the purpose of deception in legal commerce produces a counterfeit document, falsifies a genuine document or uses a counterfeit or a falsified document, shall be liable to imprisonment not exceeding five years or a fine.
(2) The attempt shall be punishable.
(3) In especially serious cases the penalty shall be imprisonment from six months to ten years. An especially serious case typically occurs if the offender 1. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of fraud or forgery; 2. causes major financial loss; 3. substantially endangers the security of legal commerce through a large number of counterfeit or falsified documents; or 4. abuses his powers or his position as a public official.
(4) Whosoever commits forgery on a commercial basis as a member of a gang whose purpose is the continued commission of offences under sections 263 to 264 or sections 267 to 269 shall be liable to imprisonment from one to ten years, in less serious cases to imprisonment from six months to five years.

document. This requirement is met if the person who appears as the author of the (hypothetical) document is not its true author. The question as to whether the elements of the offence description are fulfilled by a specific data manipulation has to be answered on a case-by-case basis depending upon the requirements of sec. 267 and sec. 269 PC.

4. Misuse of Devices

a. Object – type of device?

Does your criminal law criminalize the development of a hacker's "tool kit" or any part of it (e.g. password grabbers and key loggers, blue boxing programs, war-dialers, encryption software, program password crackers, security vulnerability scanners, packet sniffers etc.) for the unauthorized access to computer or electronic systems or transmissions?

Sec. 202c PC[50] penalizes acts preparatory to an offence under sec. 202a ("data espionage") or 202b PC ("interception of data"). The provision was introduced in the year 2007[51]. Since then the preparation of the offences in sec. 202a, 202b PC is punishable, whereas the attempt of the very same offences is not. This inconsistency of the provisions is attenuated by the fact that an attempt of the offences will most likely involve preparatory acts punishable under sec. 202c PC. Thus the provisions will only leave very few actions unpunished.

As for the penalized actions of sec. 202c PC, subsec. 1 criminalizes the production, acquirement, selling, supply, dissemination or otherwise providing of passwords or other security codes enabling access to data (defined in sec. 202a PC[52]).

Subsec. 2 criminalizes the same acts relating to software. This provision comprises the acquiring or supply of "hacker tools". Since the requirement of the aim to commit the acts punished in sec. 202a and 202b is again defined in an objective way, it is not easy to decide whether an act fulfills the elements of the offence as defined. If a company or a person only aims at testing the vulnerability of their own computer (systems) there does not exist any other way to do this but to use a "hacker's tool kit". Yet this behaviour will already amount to the actus reus of an offence under section 202c. The criminal liability of a person's behaviour will only be excluded by the lack of mens rea which in fact is not very convincing.

All of the described acts must be designed to prepare the commission of an offence under sec. 202a or 202b PC. The prerequisite of a "preparatory act" is defined in an objective manner – the character of the tool/software in itself should show its aim to commit one of the offences

[50] **Section 202c PC: Acts preparatory to data espionage and interception of data**
(1) Whosoever prepares the commission of an offence under section 202a or section 202b by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible
1. passwords or other security codes enabling access to data (section 202a(2)), or
2. software for the purpose of the commission of such an offence, shall be liable to imprisonment not exceeding one year or a fine. …

[51] 2007 Federal Law Gazette I, p- 1786.

[52] Sec. 202a subsec. 2: „…data shall only be those stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable".

of data espionage or interception of data. It suffices if the purpose of preparing an offence is one of the features of the tool among others. Thus the ambit of this definition is very far stretched – hence it is not easy to think of a tool that would not meet the preconditions of the offence established in sec. 202c PC.

The preparatory offence in sec. 202c PC is also applicable for the preparation of the offences in sec. 303a subsec. 3[53] (data tampering) and 303b subsec. 5[54] (computer sabotage).

Concerning computer fraud, preparatory acts are also punishable, sec. 263a subsec. 3 PC[55]. The offence consists of the creation of programs that aim at the commission of an offence of computer fraud. Again, the purpose of the produced program is to be determined objectively. The offence does not require the unlawful access to a computer (system) but covers the mere preparation of such access by creating a tool therefore.

Furthermore, the creation of such programs[56] is punishable under sec. 108b subsec. 2 Copyright Act[57]. This provision criminalizes unathorized access as well as preparatory acts thereto – they can consist of the creation of software programs or other "hacking tools".

---

[53] Sec. 303a subsec. 3 rules that sec. 202c PC shall apply mutatis mutendis for acts preparatory to an offence under sec. 303a.

[54] Sec. 303b subsec. 5 rules that sec. 202c PC shall apply mutatis mutendis for acts preparatory to an offence under sec. 303b.

[55] **Section 263a Computer fraud**

(1) Whosoever with the intent of obtaining for himself or a third person an unlawful material benefit damages the property of another by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorised use of data or other unauthorised influence on the course of the processing shall be liable to imprisonment not exceeding five years or a fine.

…

(3) Whosoever prepares an offence under subsection (1) above by writing computer programs the purpose of which is to commit such an act, or procures them for himself or another, offers them for sale, or holds or supplies them to another shall be liable to imprisonment not exceeding three years or a fine.

[56] **Sec. 95a Copyright Act: Protection of technological measures**

… (3) The production, import, distribution, sale, rental, advertising with a view to selling or rental and possession for commercial purposes of devices, products or components, as well as providing services, shall be prohibited which

1. are the subject-matter of sales promotions, advertising or marketing with the aim of circumventing effective technological measures, or
2. apart from circumventing effective technological measures only have a restricted economic purpose or benefit, or
3. are mostly drafted, produced, adjusted or provided in order to facilitate or make easier the circumvention of effective technological measures.

[57] **Sec. 108b Copyright Act: Infringement of technological measures and rights-management information**

(1) Any person who,

1. with the intention of enabling for himself or a third party access to a work which is protected under this Act or to other subject-matter protected under this Act or its exploitation, circumvents an effective technological measure without the consent of the rightholder, or
2. knowingly without authorisation a) removes or alters rights-management information provided by rightholders, if any of the information concerned is affixed to a copy of a work or of other protected subject-matter, or is released in the context of the communication to the public of such a work or protected subject-matter, or b) distributes, imports for distribution, broadcasts, communicates to the public or makes available to the public a work or other protected subject-matter where rights-management information was removed or altered without authorisation by doing so, has at least carelessly induced, enabled, facilitated or concealed an infringement of copyright or related rights, if the offence was not committed exclusively for the personal pri-

b. Act – public distribution/transfer to another person?

i. Does your criminal law penalize the unauthorized use of any of the hacker's tools listed above under a?

An offence specifically dedicated to the use of hacking tools in itself does not exist. Yet if the use of hacking tools serves to commit one of the crimes under sec. 202a, 202b, 263a, 303a, 303b PC, § 108b I Nr. 1 Copyright Act, it is already punishable under these provisions.

ii. Does your criminal law penalize the public distribution and/or transfer to other parties of hacked electronic information?

There is no offence penalizing the distribution of hacked information in general. However, some provisions are dedicated to the disclosure of unlawfully gained information in a certain context.

The disclosure of trade or industrial secrets to the public is punishable under sec. 17 subsec. 2 no. 2 of the Act against Unfair Competition[58]. Subsec. 2 no. 1 refers to the use of technical

---

vate use of the offender or of persons personally associated with the offender or does not relate to such use, shall be liable to imprisonment of not more than one year or a fine.
(2) Punishment shall also be imposed on any person who in violation of Article 95a (3) produces, imports, distributes, sells or rents a device, a product or component for commercial purposes.
(3) If in cases under paragraph (1) the offender acts on a commercial scale, the penalty shall be imprisonment of not more than three years or a fine.

[58] **Section 17 Act against Unfair Competition: Disclosure of trade and industrial secrets**
(1) Whoever as the employee of a business communicates, without authorisation, a trade or industrial secret with which he was entrusted, or to which he had access, during the course of the employment relationship to another person for the purposes of competition, for personal gain, for the benefit of a third party, or with the intent of causing damage to the owner of the business shall be liable to imprisonment not exceeding three years or to a fine.
(2) Whoever for the purposes of competition, for personal gain, for the benefit of a third party, or with the intent of causing damage to the owner of the business, acquires or secures, without authorisation,
1. a trade or industrial secret
a) by using technical means;
b) by creating an embodied communication of the secret; or
c) by removing an item in which the secret is embodied; or
2. without authorisation, uses or communicates to anyone a trade secret which he acquired through one of the communications referred to in subsection (1), or through an act of his own or of a third party pursuant to number 1, or which he has otherwise acquired or secured without authorization shall incur the same liability.
(3) An attempt shall incur criminal liability.
(4) In particularly serious cases the sentence shall consist in imprisonment not exceeding five years or a fine. A particularly serious case shall usually exist in circumstances where the perpetrator
1. acts on a commercial basis;
2. knows at the time of the communication that the secret is to be used abroad; or
3. himself effects a use pursuant to subsection (2), number 2, abroad.
(5) The offence shall be prosecuted upon application only, unless the criminal prosecution authority considers that it is necessary to take ex officio action on account of the particular public interest in the criminal prosecution.

means which also includes the hacking of computer systems or data communication lines. The conduct has to be committed with the aim either to gain personal profit for the perpetrator or third persons or to cause damage to the business interests of a competitor.

Furthermore it is punishable under sec. 44 subsec. 1, 43 subsec. 2 no. 1 Federal Data Protection Act to provide unlawfully gained information to others if the perpetrator does this with the aim to gain a financial benefit or to bring about a financial damage to another's detriment.

The punishability of the conduct under these provisions does not refer to the fact that the information was gained by the "hacking" of a computer (system), but it is triggered by the specific character of the information. The provisions protect the victim's specific financial or other business interests related to the disclosed data. In general, the dissemination of data is punishable if a specific interest of its confidentiality is violated.

c. Possession?

Does your criminal law criminalize the possession of a hacker's „tool kit" or any part of it (e.g. password grabbers and key loggers, blue boxing programs, war-dialers, encryption software, program password crackers, security vulnerability scanners, packet sniffers etc.) for the unauthorized access to computer or electronic systems or transmissions?

The mere possession of a hacker's tool kit is not criminalized specifically in the PC. Yet since the unlawful acquisition of data is criminalized in sec. 202a, 202b, 263a PC, the later possession is criminalized indirectly[59]. Nevertheless, sec. 111a subsec. 1 no. 1b Copyright Act[60] makes it an administrative offence to possess devices described in sec. 95a III Copyright Act[61].

(b) Privacy[62]

(6) Section 5, number 7, of the Criminal Code shall apply mutatis mutandis.

[59] *Ernst,* Neue Juristische Wochenschrift 2007, pp. 2661, 2663.

[60] **Article 111a Copyright Act: Regulatory fining provisions**
(1) Any person who
1. in violation of Article 95a (3)
a) sells, rents or distributes a device, a product or component outside the group of people with whom the offender is personally associated, or
b) for commercial purposes possesses, advertises for sale or rental or provides a service in respect of a device, a product or a component,
2. in violation of Article 95b (1), first sentence, does not provide necessary means, or
3. in violation of Article 95d (2), first sentence, does not or does not fully label works or other protected subject-matter,
shall be deemed to have committed a regulatory offence administrative offence.
(2) In cases under paragraph (1) items 1 and 2, the regulatory offence may be sanctioned with a regulatory fine of not more than 50,000 euro and in other cases with a regulatory fine of not more than 10,000 euro.

[61] **Sec. 95a Copyright Act, see** footnote 56.

[62] Please note that the following description only gives an account of federal laws. The German law on data protection is to some extent subject to laws of the federal states of Germany. If a state law exists on a certain

1. Violation of Secrecy of Private Data

a. Object – type of private data?

(Note: private data are data that belong to people's private life but do not identify or make it possible to identify a person, e.g., civil status, sexual orientation, health status, buying habits or preferences)

i. Do your country's laws require that data collectors disclose their information practices before collecting private information from consumers like, for example, which information is used, how it is collected and for what purposes, whether it is shared with others or whether consumers have any control over the disclosure of their private data?

Yes, there are several regulations on the disclosure of data collection policies in German law. German law specifies different regulations concerning the specific context of data collection measures.

Sec. 4 subsec. 2 Federal Data Protection Act[63] rules that personal data are to be collected with the help of the person who holds the data ("data subject"). This demands knowledge and consent of the "data subject" as well as the participation of this person in the process of collecting the data[64]. The prerequisite is meant to make sure that the person's right to informational self-determination is respected. The data subject should know if someone collects any data about him/her[65]. A right to collecting data without the knowledge of the data subject is granted only in exceptional cases.

---

area it overrides the regelutation of the federal law of the Federal Data Protection Act. However, since the Federal Data Protection Act represents the "German" law on data protection, the following explanations are restricted to this statute.

[63] **Section 4 Federal Data Protection Act: Lawfulness of data collection, processing and use**
(1) The collection, processing and use of personal data shall be lawful only if permitted or ordered by this Act or other law, or if the data subject has provided consent.
(2) Personal data shall be collected from the data subject. They may be collected without the data subject's participation only if
1. allowed or required by law, or
2. a) the data must be collected from other persons or bodies due to the nature of the administrative task to be performed or the commercial purpose, or
b) collecting the data from the data subject would require disproportionate effort and there are no indications that overriding legitimate interests of the data subject would be adversely affected.
(3) If personal data are collected from the data subject, the controller shall inform him/her as to
1. the identity of the controller,
2. the purposes of collection, processing or use, and
3. the categories of recipients only where, given the circumstances of the individual case, the data subject need not expect that his/her data will be transferred to such recipients, unless the data subject is already aware of this information. If personal data are collected from the data subject pursuant to a law requiring the provision of such information, or if providing this information is required for the granting of legal benefits, the data subject shall be informed that providing this information is required or voluntary, as the case may be. The law and the consequences of refusing to provide information shall be explained to the data subject as necessary in the individual case.

[64] Simitis-*Sokol (Commentary on the Federal Data Protection Act; hereinafter: "Simitis-author"),* § 4 marginal no. 23; *Gola/Schomerus,* Commentary on the Federal Data Protection Act (hereinafter: "Gola/Schomerus"), § 4, marginal no. 21.

[65] *Gola/Schomerus,* § 4 marginal no. 21; Simitis-*Sokol,* § 4 marginal no. 20.

If data are collected with the help of their subject, sec. 4 subsec. 3 Federal Data Protection Act[66] is admissible. The provision requires that the data subject is informed about

1. the identity of the data controller,

2. the purposes of data collection, processing or use, and

3. the categories of recipients only where, given the circumstances of the individual case, the data subject need not expect that his/her data will be transferred to such recipients, unless the data subject is already aware of this information.

This duty to inform the data subject is meant to make sure that he/she can decide on the disclosure of the personal data.[67] The data subject has to be informed before the data is collected.[68] In case the data subject already knows about the ongoing data collecting, no further information is needed.[69] This is also true if the collecting of data is only permissible with the data subject's consent. Since an effective consent depends upon full knowledge of the facts, a further notification of a collecting of data is superfluous if the data can only be collected with a previous consent of the data subject.[70]

Sec. 4 subsec. 3 Federal Data Protection Act rules, that

"if personal data are collected from the data subject pursuant to a law requiring the provision of such information, or if providing this information is required for the granting of legal benefits, the data subject shall be informed that providing this information is required or voluntary, as the case may be. The law and the consequences of refusing to provide information shall be explained to the data subject as necessary in the individual case."

In case the data subject is legally obliged to provide the data or to cooperate in the collecting of data he or she has to be informed about his duty to do so or – if so – about the voluntariness of his or her cooperation, sec. 4 subsec. 3 Federal Data Protection Act[71].

If the collecting of data is meant to serve the collector's business interests, specific information duties have to be complied with. Moreover the data subject has a right to object to the data collecting, sec. 28 subsec. 4 Federal Data Protection Act[72].

---

[66] **Sec. 4 Federal Data Protection Act**, see footnote 63.
[67] *Gola/Schomerus,* § 4, Rn. 29; *Ambs,* in Erbs/Kohlhaas, Strafrechtliche Nebengesetze, D 25, BDSG, § 4, Rn. 16.
[68] *Gola/Schomerus,* § 4, Rn. 29; Simitis-*Sokol,* § 4, Rn. 56.
[69] *Gola/Schomerus,* § 4, Rn. 36 ff; Simitis-*Sokol,* § 4, Rn. 40.
[70] *Gola/Schomerus,* § 4, Rn. 40.
[71] See footnote 63.
[72] **Section 28 Federal Data Protection Act**: Collection and recording of data for own commercial purposes … (4) If the data subject lodges an objection with the controller regarding the processing or use of his or her data for advertising purposes or market or opinion research, processing or use for these purposes shall be unlawful. In approaching the data subject for the purpose of advertising or market or opinion research, and in the cases of subsection 1 first sentence no. 1 also when creating a legal or quasi-legal obligation, the data subject shall be informed of the identity of the controller and of the right to object under the first sentence; where the party approaching the data subject uses the data subject's personal data recorded by a body unknown to him or her, the approaching party shall also ensure that the data subject may obtain information about the source of the data. If the data subject lodges an objection with the third party to which the data were transferred in connection with purposes under subsection 3 as to the processing or use for purposes of advertising or market

If the collecting or recording of data is administered without the subject's knowledge he or she is to be informed afterwards by the collector of the data, sec. 19a (collection by public bodies), 33 (collection by private bodies) Federal Data Protection Act[73]. The information has to be provided without undue delay[74]. The provisions leave certain exceptions from the information duties[75].

---

or opinion research, the third party shall block the data for these purposes. In the cases of subsection 1 first sentence no. 1, the requirements as to the form of the objection may not be stricter than for the creation of a legal or quasi-legal obligation.

[73] **Section 19a Federal Data Protection Act: Notification**

(1) If data are collected without the data subject's knowledge, he or she shall be notified of such recording, the identity of the controller and the purposes of collection, processing or use. The data subject shall also be notified of recipients or categories of recipients except where he or she must expect transfer to such recipients. If a transfer is planned, notification shall be provided no later than the first transfer.

Section 33 Federal Data Protection Act: Notification of the data subject

(1) If personal data are recorded for own purposes for the first time without the data subject's knowledge, the data subject shall be notified of such recording, the type of data, the purpose of collection, processing or use and the identity of the controller. If personal data are commercially recorded for the purpose of transfer without the data subject's knowledge, the data subject shall be notified of their initial transfer and of the type of data transferred. In the cases covered by the first and second sentences above, the data subject shall also be notified of the categories of recipients, where, given the circumstances of the individual case, the data subject need not expect that his/her data will be transferred to such recipients.

[74] Simitis-*Mallmann,* § 19a marginal no. 27; Simitis-*Dix,* § 33 marginal no. 41.

[75] **Sec. 19a Federal Data Protection Act**

(2) Notification shall not be required if

1. the data subject already has this information,
2. notifying the data subject would involve a disproportionate effort, or
3. recording or transfer of personal data is expressly laid down by law.

Sec. 33 Federal Data Protection Act

(2) Notification shall not be required if

1. the data subject has become aware of the recording or transfer by other means,
2. the data were recorded only because they may not be erased due to legal, statutory or contractual provisions on retention, or only for purposes of monitoring data protection or safeguarding data, and providing information would require a disproportionate effort,
3. the data must be kept secret by law or due to the nature of the data, namely due to the overriding legal interests of a third party,
4. recording or transfer is expressly laid down by law,
5. recording or transfer is necessary for the purposes of scientific research and notification would require a disproportionate effort,
6. the responsible public body has informed the controller that disclosure of the data would threaten the public security or order or otherwise be detrimental to the Federation or a Land, or
7. the data were recorded for own purposes and

a) were acquired from generally accessible sources and notification would require a disproportionate effort due to the large number of cases concerned, or

b) notification would seriously endanger the commercial purposes of the controller, unless the interest in notification overrides this danger,

8. The data were commercially recorded for the purpose of transfer, and

a) were acquired from generally accessible sources, where they related to the persons who published the data, or

b) the data are compiled in lists or otherwise summarized (Section 29 (2) second sentence) and notification would require a disproportionate effort due to the large number of cases concerned,

9. data acquired from generally accessible sources recorded commercially for the purpose of market or opinion research and notification would require a disproportionate effort due to the large number of cases concerned.

For data collection which has taken place with the consent of the data subject, special information obligations are established in sec. 4a subsec. 1 Federal Data Protection Act[76]. The data subject shall be informed about the purpose of the data collection and about the way the data is supposed to be used in the future. Since the data subject's consent has to be based upon his or her own free decision, all the information needed for a fully-informed decision has to be supplied in advance. This includes information on the consequences of a denial of the requested consent. Moreover, the data subject is to be informed about his/her right to withdraw a formerly given consent, sec. 28 subsec. 3a Federal Data Protection Act[77].

Concerning the surveillance of public places, specific information duties are to be fulfilled, sec. 6b, 6c Federal Data Protection Act[78].

ii. Do your country's laws require companies and entities doing business on the internet to inform consumers of the identity of who is collecting the data, if the provision of the requested data is voluntary or required and the steps taken by the data collector to ensure the confidentiality, the integrity and the quality of the data?

[76] **Section 4a Federal Data Protection Act: Consent**
(1) Consent shall be effective only when based on the data subject's free decision. Data subjects shall be informed of the purpose of collection, processing or use and, as necessary in the individual case or on request, of the consequences of withholding consent. Consent shall be given in writing unless special circumstances warrant any other form. If consent is to be given together with other written declarations, it shall be made distinguishable in its appearance.

[77] **Sec. 28 Federal Data Protection Act**: (3a) If consent under section 4a (1) third sentence is given in a form other than writing, the controller shall provide the data subject with written confirmation of the substance of the consent unless consent was given in electronic form and the controller ensures that the declaration of consent is recorded and the data subject can access and revoke it at any time with future effect. If consent is to be given together with other written declarations, it shall be made distinguishable in its printing and format. *Taeger,* DuD 2010, 246, 248.

[78] **Section 6b Federal Data Protection Act: Monitoring of publicly accessible areas with optic-electronic devices**
(1) Monitoring publicly accessible areas using optic-electronic devices (video surveillance) shall be lawful only as far as necessary
1. for public bodies to perform their duties,
2. to exercise the right to determine who shall be allowed or denied access, or
3. to pursue legitimate interests for specifically defined purposes, and there are no indications of overriding legitimate interests of the data subject.
(2) Suitable measures shall be taken to make clear that the area is being monitored and to identify the controller.
Section 6c Federal Data Protection Act: Mobile storage and processing media for personal data
(1) A body which issues mobile storage and processing media for personal data or which applies to such media a procedure for the automated processing of personal data which runs wholly or partly on such media, or which alters or makes available such a procedure shall
1. inform the data subject of its identity and address,
2. explain to the data subject, in generally understandable terms, how the medium works, including the type of personal data to be processed,
3. inform the data subject how to exercise his or her rights under Sections 19, 20, 34 and 35, and
4. inform the data subject what measures are to be taken in case the medium is lost or destroyed, if the data subject is not already aware of this.

Even if the provision of personal data is voluntary or required to assure the confidentiality or integrity of data, basically the same rules on information duties as mentioned above apply. However, sec. 4 subsec. 3, 19a subsec. 2, 33 subsec. 2 Federal Data Protection Act[79] allow for exceptions from these rules, for example if the information is collected in order to monitor data protection or to safeguard data, and if the providing of information would require a disproportionate effort, sec. 33 subsec. 2 no - 2 Federal Data Protection Act. This exception is of very low practical relevance for the data usually have to be recorded in advance – and this already makes a notification necessary[80].

iii. Do your country's laws require websites to display a privacy policy and explain how personal information will be used before consumers enter the purchase process or any other transactions for which they must provide sensitive information?

Basically, the same regulations on information and notification obligations as ruled in sec. 4 subsec. 3 Federal Data Protection Act as well as similar regulations (for example sec. 93 Telecommunications Act[81]) apply. As far as data are collected only **for the purpose of concluded contracts**, there is no need to indicate the purpose of the data collecting. Furthermore, it is not necessary to point out the voluntariness of the disclosure of personal data. As soon as further information is collected, the duties to provide information apply again. What is more, it is forbidden to demand the customer's consent to further data collecting that is not needed in order to conclude the current contract. This prohibition can generally be derived from sec. 242 of the German Civil Code[82]. Furthermore, certain specific provisions in the German Data Protection Law establish this so-called „Kopplungsverbot", e.g. sec. 28 Federal Data Protection Act[83].

The Federal Data Protection Act does not sepcify in which way exactly the provision of information shall be performed. It is only necessary that the data subject is enabled to properly understand the information provided. Accordingly, sec. 13 Telemedia Law and sec. 93 subsec. 1 Telecommunications Act require that the notification shall be generally understandable.

[79] Sec. 33 subsec. 2 see footnote 75.

[80] *Gola/Schomerus,* § 33 marginal no. 32; *Ambs,* in Erbs/Kohlhaas, Strafrechtliche Nebengesetze, D 24, BDSG, § 33, marginal no. 13; vgl. auch Simitis-*Dix,* § 33, marginal no. 70.

[81] **Section 93 Telecommunications Act**: Duty to Provide Information
When concluding contracts, service providers shall inform their subscribers of the nature, extent, place and purpose of the collection and use of personal data in such a way that the subscribers are given notice, in readily comprehensible form, of the basic data processing facts. The attention of subscribers shall also be drawn to the choices and options permitted. Users shall be informed by the service provider by means of generally available information about the collection and use of personal data. The right to provision of information as set out in the Federal Data Protection Act remains unaffected.

[82] **Section 242 Civil Code: Performance in good faith**
An obligor has a duty to perform according to the requirements of good faith, taking customary practice into consideration.

[83] See for example: **Sec. 28 Federal Data Protection Act: Collection and recording of data for own commercial purposes**
(3b) The controller may not make the conclusion of a contract dependent on the data subject's consent under subsection 3 first sentence, if access to equivalent contractual benefits is impossible or unreasonable without providing consent. Consent provided under such circumstances shall be invalid.

This includes the rule that the use of technical or legal terms should be avoided as far as possible[84]. Apart from this, if the collecting of data is done in written form, the same is required for the provision of the notification about the data collection[85]. Websites shall indicate Data Protection Statements by clear and easily recognizable links[86]. Since it suffices that the link is indicated, this is the most common way used for complying with data protection rules.

iv. Does the criminal law of your country penalize failing to provide the disclosures mentioned above (a.i; a.ii and a.iii)?

The breach of the duty to provide information in sec. 4 subsec. 3 Federal Data Protection Act does neither amount to a criminal nor to an administrative offence. Under certain circumstances, however, the breach of this duty may lead to the unlawfulness of the data collecting – which does in fact lead to an administrative offence under sec. 43 subsec. 2 no. 1 Federal Data Protection Act[87].

In general however the data subject has to seek for reparation under the civil law in case of a failure to provide information. This is always connected to the claim of a material (financial) damage, which in most of the cases will not be given.

The failure to indicate the data subject's right to object to the data collection (sec. 28 subsec. 4 Federal Data Protection Act) is subject to an administrative offence under sec. 43 subsec. 1 no. 3 Federal Data Protection Act[88].

b. Act – illegal use and transfer/distribution?

i. Does the criminal law of your country define the illegal transfer and distribution of private data?

Yes, this behaviour is criminalized in certain specific provisions. But there is no basic provision that criminalizes illegal transfer and distribution of private data in general.

[84] *Taeger,* DuD 2010, 246, 249.
[85] *Ambs,* in Erbs/Kohlhaas, Strafrechtliche Nebengesetze, D 25, BDSG, § 4 marginal no. 18; *Gola/Schomerus,* § 4, marginal no. 31.
[86] *Arning/Haag,* in Heise Online-Recht, C. Kap. II., marginal no. 40.
[87] **Sec. 43 Data Protection Act: Administrative offences**
(1) An administrative offence shall be deemed to have been committed by anyone who, whether intentionally or through negligence
… 8. in violation of Section 33 (1) fails to notify the data subject, or fails to do so correctly or completely, …
[88] **Sec. 43 Data Protection Act: Administrative offences**
(1) An administrative offence shall be deemed to have been committed by anyone who, whether intentionally or through negligence …
3. in violation of Section 28 (4) second sentence fails to notify the data subject, or fails to do so correctly or within the prescribed time limit, or fails to ensure that the data subject may obtain the relevant information, …

ii. Does the criminal law of your country penalize the illegal use, transfer and/or distribution of private data?

Sec. 43 subsec. 2 no. 1 Fedeal Data Protection Act[89] makes it an administrative offence to collect or process personal data without authorization of the data subject. It has to be pointed out that the offence description is met not only in case of intent but also in case of negligent behaviour.

The collection of data is defined as acquisition of data on the data subject in sec. 3 subsec. 3 Federal Data Protection Act. The processing of data is defined as the recording, alteration, transfer, blocking and erasure of personal data in sec. 3 subsec. 4 Federal Data Protection Act[90]. The unauthorized use of personal data is not encompassed by the offence description[91]. Only if the specific requirements of sec. 43 subsec. 2 no. 5, 5b Federal Data Protection Act[92] are met, the requirements of a specific administrative offence are satisfied. Apart from this, subsec. 2[93] enlists specific violations of obligations concerning the collecting or processing of

[89] **Sec. 43 Data Protection Act: Administrative offences**
(2) An administrative offence shall be deemed to have been committed by anyone who, whether intentionally or through negligence
1. collects or processes personal data which are not generally accessible without authorization,

[90] The provision rules further:
Sec. 3 subsec. 4 Federal Data Protection Act
Specifically, irrespective of the procedures applied,
1. "recording" shall mean the entry, recording or preservation of personal data on a storage medium so that they can be further processed or used,
2. "alteration" shall mean the modification of the substance of recorded personal data,
3. "transfer" shall mean the disclosure of personal data recorded or obtained by data processing to a third party either
a) through transfer of the data to a third party, or
b) by the third party inspecting or retrieving data available for inspection or retrieval,
4. "blocking" shall mean the identification of recorded personal data so as to restrict their further processing or use,
5. "erasure" shall mean the deletion of recorded personal data.

[91] *Gola/Schomerus,* § 43 marginal no. 20.

[92] **Sec. 43 Federal Data Protection Act: Administrative offences**
(2) An administrative offence shall be deemed to have been committed by anyone who, whether intentionally or through negligence
5. in violation of Section 16 (4) first sentence, Section 28 (5) first sentence, also in conjunction with Section 29 (4), Section 39 (1) first sentence or Section 40 (1), uses transferred data for other purposes,
5 b. in violation of Section 28 (4) first sentence processes or uses data for purposes of advertising or market or opinion research, …

[93] **Sec. 43 Federal Data Protection Act: Administrative offences**
(2) An administrative offence shall be deemed to have been committed by anyone
who, whether intentionally or through negligence
1. collects or processes personal data which are not generally accessible without authorization,
2. makes available personal data which are not generally accessible by means of automated retrieval without authorization,
3. retrieves personal data which are not generally accessible without authorization, or obtains such data for themselves or others from automated processing operations or non-automated files without authorization,
4. obtains transfer of personal data which are not generally accessible by providing false information,
5. in violation of Section 16 (4) first sentence, Section 28 (5) first sentence, also in conjunction with Section 29 (4), Section 39 (1) first sentence or Section 40 (1), uses transferred data for other purposes,
5 a. in violation of Section 28 (3b) makes the conclusion of a contract dependent on the consent of the data subject,

personal data that amount to adminstrative offences. If the perpetrator aims at financial benefits for him or another or if he aims at damaging another's financial interests, the violation of sec. 43 amounts to a criminal offence under sec. 44 subsec. 1 Federal Data Protection Act[94].

Sec. 149 Telecommunications Act[95] makes it an administrative offence to use data that were produced by the use of telecommunication devices. The provision applies if data are collected or processed and these acts are defined in the same way as in sec. 43, 3 Federal Data Protection Act.

c. Justification?

i. Under which conditions does your country's law allow for the authorized collection, processing, transfer and distribution of private data?

In general the collection, processing or use of personal data is forbidden in Germany. However, sec. 4 Federal Data Protection Act rules that in certain situations the collecting, processing and use of personal data is lawful. That is, if a specific provision allows for the collection in a certain context, if the data subject permitted the collection or if the data collection is ordered by law[96]. Thus sec. 4 subsec. 1 Federal Data Protection Act articulates the main principle of

---

5 b. in violation of Section 28 (4) first sentence processes or uses data for purposes of advertising or market or opinion research,
6. in violation of Section 30 (1) second sentence, Section 30a (3) third sentence or Section 40 (2) third sentence combines a feature referred to there with specific information, or
7. in violation of Section 42a first sentence, fails to notify or fails to do so correctly, completely or within the prescribed time limit.

[94] **Section 44 Federal Data Protection Act: Criminal offences**
(1) Anyone who wilfully commits an offence described in Section 43 (2) in exchange for payment or with the intention of enriching him-/herself or another person, or of harming another person shall be liable to imprisonment for up to two years or to a fine.

[95] **Section 149 Telecommunications Act: Administrative Fines Provisions**
(1) An administrative offence is deemed to have been committed by any person who, intentionally or negligently,
16. in contravention of section 95(2) or section 96(2) sentence 1 or subsection (3) sentence 1, uses data; …

[96] **Section 4 Federal Data Protection Act: Lawfulness of data collection, processing and use**
(1) The collection, processing and use of personal data shall be lawful only if permitted or ordered by this Act or other law, or if the data subject has provided consent.
(2) Personal data shall be collected from the data subject. They may be collected without the data subject's participation only if
1. allowed or required by law, or
2. a) the data must be collected from other persons or bodies due to the nature of the administrative task to be performed or the commercial purpose, or
b) collecting the data from the data subject would require disproportionate effort and there are no indications that overriding legitimate interests of the data subject would be adversely affected.
(3) If personal data are collected from the data subject, the controller shall inform him/her as to
1. the identity of the controller,
2. the purposes of collection, processing or use, and
3. the categories of recipients only where, given the circumstances of the individual case, the data subject need not expect that his/her data will be transferred to such recipients, unless the data subject is already aware of

the German law on data protection: The collecting of personal data is forbidden in the first place. Nevertheless data collecting/processing/usage can be lawful if specific legal permissions allow for the particular data collecting/processing/usage.[97] Provisions allowing for a collection of data can be found in various statutes and are related to various contexts – some of those provisions are more specific than the general rules in the Federal Data Protection Act and take precedence over them, sec. 1 subsec. 3 Federal Data Protection Act.[98] The general rules of the Federal Data Protection Act are to be found in chapter 2 and 3 of this Act. Chapter 2 contains provisions on data collection by public bodies, chapter 3 refers to the collection of data by private bodies. If no provision allows for the collection of data, it can nevertheless be lawful if it is authorized by the data subject's consent. The prerequisites of a valid consent are stipulated in sec. 4a Federal Data Protection Act.[99]

Specific regulations concerning telecommunication are to be found in sec. 91 ss. Telecommuncations Act. The general prohibition of data collecting if not authorized by special regulations or the data subject's consent applies here as well[100]. The specific regulations of the Telecommunications Act take precedence over the rules of the Federal Data Protection Act.

ii. What standard of need is required for an authorized collection and/or distribution (compelling, important, reasonable, convenient)?

There are three general principles ruling the lawful collecting of data:

1. The *necessity* of the demanded data is the basic prerequisite of a lawful data collecting[101]. The necessity in general is one of the basic principles of administrative procedures. It is of special interest in the field of data collection and is stated in the Federal Data Protection Act

---

this information. If personal data arecollected from the data subject pursuant to a law requiring the provision of such information, or if providing this information is required for the granting of legal benefits, the data subject shall be informed that providing this information is required or voluntary, as the case may be. The law and the consequences of refusing to provide information shall be explained to the data subject as necessary in the individual case.

[97] *Gola/Schomerus,* § 4 marginal no. 3; siehe auch Simitis-*Sokol,* § 4 marginal no. 2.

[98] *Gola/Schomerus,* § 4 margial no. 7.

[99] **Section 4a Federal Data Protection Act: Consent**

(1) Consent shall be effective only when based on the data subject's free decision. Data subjects shall be informed of the purpose of collection, processing or use and, as necessary in the individual case or on request, of the consequences of withholding consent. Consent shall be given in writing unless special circumstances warrant any other form. If consent is to be given together with other written declarations, it shall be made distinguishable in its appearance.

Sec. 28 subsec. 3a Federal Data Protection Act contains even more prerequisites for a valid consent related to the collection of personal data by private bodies:

„(3a) If consent under Section 4a (1) third sentence is given in a form other than writing, the controller shall provide the data subject with written confirmation of the substance of the consent unless consent was given in electronic form and the controller ensures that the declaration of consent is recorded and the data subject can access and revoke it at any time with future effect. If consent is to be given together with other written declarations, it shall be made distinguishable in its printing and format."

[100] *Eckhardt,* in Spindler/Schuster, Recht der elektronischen Medien, TKG, § 91 marginal no. 3.

[101] E.g. sec. 13 I Federal Data Protection Act: (1) Collecting personal data shall be lawful when the knowledge of such data is necessary for the controller to perform its tasks.

as well as in many specific statutes for particular fields of the law. The exact meaning of the term „necessity" differs depending on the context in which it is used[102]. Thus, necessity has to be interpreted in regard to the context, the character of the collected data and the specific interest in the confidentiality of the relevant data.

2. The second condition is the *principle of data avoidance and data economy*, sec. 3a Federal Data Protection Act[103]. Yet this principle is only established as an objective. As soon as the prerequisite of necessity is met, the data collection is lawful. It will not lead to the unlawfulness of the data collection if the principle of data avoidance and economy was violated.

3. Finally the *principle of purpose* has to be respected. This means that the collection of data can only be legitimized if it serves specified and explicit purposes, „Zweckbindungsgrundsatz". Retention of data cannot be legitimized.

As far as data collection by public bodies is concerned, the principle of necessity is explicitly established in sec. 13, 14 Federal Data Protection Act[104].

---

[102] Simitis-*Sokol,* § 13, Rn. 25; *Ambs,* in Erbs/Kohlhaas, Strafrechtliche Nebengesetze, D 25, BDSG, § 13, Rn. 2.

[103] **Section 3a Federal Data Protection Act: Data reduction and data economy**
Personal data shall be collected, processed and used, and data processing systems shall be chosen and organized in accordance with the aim of collecting, processing and using as little personal data as possible. In particular, personal data shall be rendered anonymous or aliased as allowed by the purpose for which they are collected and/or further processed, and as far as the effort required is not disproportionate to the desired purpose of protection.

[104] **Section 13 Federal Data Protection Act: Data collection**
(1) Collecting personal data shall be lawful when the knowledge of such data is necessary for the controller to perform its tasks.
(1 a) If personal data are collected from a private body rather than from the data subject, this body shall be informed of the legal provision requiring the supply of information or that such supply is voluntary.
(2) Collecting special categories of personal data (Section 3 (9)) shall be lawful only where
1. allowed by law or urgently required for reasons of important public interest,
2. the data subject has given his consent in accordance with Section 4a (3),
3. necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent,
4. data are involved which the data subject has manifestly made public,
5. necessary to prevent a significant threat to the public security,
6. urgently required to prevent significant disadvantages to the common good or to preserve significant concerns of the common good,
7. required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where these data are processed by health professionals or other persons subject to the obligation of professional secrecy,
8. necessary for the purposes of scientific research, where the scientific interest in carrying out the research project significantly outweighs the data subject's interest in ruling out the possibility of collection and the purpose of the research cannot be achieved in any other way or would require a disproportionate effort, or
9. required for compelling reasons of defence or to fulfil supranational or intergovernmental obligations of a public body of the Federation in the field of crisis management or conflict prevention or for humanitarian measures.

Section 14 Federal Data Protection Act: Recording, alteration and use of data
(1) The recording, alteration or use of personal data shall be lawful when required to carry out the tasks for which the controller is responsible and for the purpose for which the data were collected. If no prior collection took place, the data may be altered or used only for the purpose for which they were recorded.
(2) Recording, alteration or use for other purposes shall be lawful only if
1. allowed or required by law,

Apart from these prerequisites of a lawful data collection, the requirements of sec. 4 subsec. 1 Federal Data Protection Act have to be respected. The provision declares a general prohibition of the collection of personal data, unless it is specifically legitimized by law. The two restrictions on data collection postulate not only the restrictive interpretation of the provisions on a lawful data collection but also confirm the principles of data avoidance and data economy. A collection of personal data has to be necessary for the performance of public services. It is necessary only if public services could not in the requested or in a lawful way be performed without the demanded data[105]. If no specific provision on a lawful data collection exists, it has to be analysed for each and every case how far a lawful data collection might reach.

As far as data collection for private business is concerned, the principle of necessity is established in sec. 28 subsec. 1 Federal Data Protection Act[106]. There has to exist an immediate

---

2. the data subject has given his consent,
3. this is clearly in the interest of the data subject and there is no reason to assume that the data subject would refuse to give his consent if he knew of such other purpose,
4. information supplied by the data subject must be checked because there is reason to believe this information is incorrect,
5. the data are generally accessible or the controller would be allowed to publish them, unless the data subject has a clear and overriding legitimate interest in ruling out the possibility of a change of purpose,
6. required to prevent significant disadvantages to the common good or a threat to public security or to preserve significant concerns of the common good,
7. required to prosecute criminal or administrative offences, to enforce sentences or measures within the meaning of Section 11 (1) no. 8 of the Criminal Code or of reformatory or disciplinary measures within the meaning of the Youth Courts Act or to enforce decisions on fines,
8. required to prevent a serious infringement of the rights of another person, or
9. necessary for the purposes of scientific research, where the scientific interest in carrying out the research project significantly outweighs the data subject's interest in ruling out the possibility of collection and the purpose of the research cannot be achieved in any other way or would require a disproportionate effort.

(3) Processing or use for the purpose of exercising supervisory and monitoring authority, of auditing or conducting organizational studies for the controller shall not constitute processing or use for other purposes. This shall also apply to processing or use for training or examination purposes by the controller, unless the data subject has overriding legitimate interests.

(4) Personal data recorded exclusively for purposes of monitoring data protection, safeguarding data or ensuring proper operation of a data processing system may only be used for these purposes.

(5) Recording, altering or using special categories of personal data (Section 3 (9)) for other purposes shall be lawful only if

1. the conditions are met which would allow collection under Section 13 (2) nos. 1 through 6 or 9, or
2. necessary for the purposes of scientific research, where the public interest in carrying out the research project significantly outweighs the data subject's interest in ruling out the possibility of collection and the purpose of the research cannot be achieved in any other way or would require a disproportionate effort.

In weighing the public interest under the first sentence, no. 2, special attention shall be paid to the scientific interest in the research project.

(6) Recording, altering or using special categories of personal data (Section 3 (9)) for the purposes referred to in Section 13 (2) no. 7 shall be subject to the obligation of secrecy which applies to the persons referred to in Section 13 (2) no. 7.

[105] Simitis-*Sokol,* § 13 maginal no. 25 f.; *Gola/Schomerus,* § 13 marginal no. 3.

[106] **Section 28 Federal Data Protection Act: Collection and recording of data for own commercial purposes**

(1) The collection, recording, alteration or transfer of personal data or their use as a means to pursue own commercial purposes shall be lawful

1. if necessary to create, perform or terminate a legal obligation or quasi-legal obligation with the data subject,
2. as far as necessary to safeguard legitimate interests of the controller and there is no reason to assume that the data subject has an overriding legitimate interest in ruling out the possibility of processing or use, or

connection to the purpose of the underlying contract[107]. This has to be considered on the basis of the specific contract – again a specific assessment of each single case is to be performed[108]. Necessity has to be interpreted as an interest of the involved persons in the data collection that can be met by the data collection. It is not necessary that the data collection be mandatory for the contract, it suffices if the data collection serves the interests of the involved parties and a waiver would not be reasonable[109].

2. Violation of professional confidentiality

a. Object – type of private data?

i. Do your country's law require that professionals disclose:
- Their information collection and management practices before collecting personal information from their patients or clients;
- Their disclosure practices;
- Their professional ethical obligations;
- And whether patients or clients have any control over the disclosure of their personal data?

If personal data are collected the general obligations of notification and information (sec. 4 subsec. 3, 4a Federal Data Protection Act[110]) apply – see (C) (b) 1. a. i.

Apart from this, special provisions can apply with respect to the specific areas of data collection. If special provisions exist, they take precedence over the regulations of the Federal Data Protection Act, sec. 1 subsec. 3 Federal Data Protection Act. For example there are specific provisions concerning the data collection by (pension or other) insurance companies.

ii. Which data are specifically protected, if any?

Generally, personal data are protected by the provisions of the Federal Data Protection Act. Personal data are defined as any information concerning the personal or material circumstances of an identified or identifiable natural person ("data subject"), sec. 3 subsec. 1 Federal Data Protection Act.

---

3. if the data are generally accessible or the controller would be allowed to publish them, unless the data subject has a clear and overriding legitimate interest in ruling out the possibility of processing or use. When personal data are collected, the purposes for which the data are to be processed or used shall be specifically defined.

[107] *Gola/Schomerus,* § 28 marginal no. 15; Simitis-*Simitis,* § 28 marginal no. 57; *Ambs,* in Erbs/Kohlhaas, Strafrechtliche Nebengesetze, D 25, BDSG, § 28 marginal no. 4.

[108] *Tinnefeld/Buchner/Petri,* Einführung in das Datenschutzrecht, S. 364; *Ambs,* in Erbs/Kohlhaas, Strafrechtliche Nebengesetze, D25, BDSG, § 28 marginal no. 4.

[109] *Gola/Schomerus,* § 28 marginal no. 15.

[110] See footnote 99.

Apart from this, specific obligations of professional secrecy apply. This is true for members of public service agencies concerning all information they gain pertaining to their professional duties. The same applies for medical professionals: They are obliged to confidentiality concerning all information they gain in their professional function. Specific duties of professional secrecy apply as well for lawyers and tax counsellors. Sec. 203 PC criminalizes the disclosure of personal secrets the perpetrator got to know in his professional function[111]. Secrets are de-

[111] **Section 203 PC: Violation of private secrets**
(1) Whosoever unlawfully discloses a secret of another, in particular, a secret which belongs to the sphere of personal privacy or a business or trade secret, which was confided to or otherwise made known to him in his capacity as a
1. physician, dentist, veterinarian, pharmacist or member of another healthcare profession which requires state-regulated education for engaging in the profession or to use the professional title;
2. professional psychologist with a final scientific examination recognised by the State;
3. attorney, patent attorney, notary, defence counsel in statutorily regulated proceedings, certified public accountant, sworn auditor, tax consultant, tax agent, or organ or member of an organ of a law, patent law, accounting, auditing or tax consulting firm in the form of a company;
4. marriage, family, education or youth counsellor as well as addiction counsellor at a counselling agency which is recognised by a public authority or body, institution or foundation under public law;
4a. member or agent of a counselling agency recognised under section 3 and section 8 of the Act on Pregnancies in Conflict Situations;
5. a state-recognised social worker or state-recognised social education worker; or
6. member of a private health, accident or life insurance company or a private medical, tax consultant or attorney invoicing service,
shall be liable to imprisonment not exceeding one year or a fine.
(2) Whosoever unlawfully discloses a secret of another, in particular, a secret which belongs to the sphere of personal privacy or a business or trade secret, which was confided to or otherwise made known to him in his capacity as a
1. public official;
2. person entrusted with special public service functions;
3. person who exercises duties or powers under the law on staff employment representation;
4. member of an investigative committee working for a legislative body of the Federation or a state, another committee or council which is not itself part of the legislative body, or as an assistant for such a committee or council;
5. publicly appointed expert who is formally obliged by law to conscientiously fulfil his duties, or
6. person who is formally obliged by law to conscientiously fulfil his duty of confidentiality in the course of scientific research projects,
shall incur the same penalty. Particular statements about personal or material relationships of another which have been collected for public administration purposes shall be deemed to be equivalent to a secret within the meaning of the 1st sentence above; the 1st sentence above shall not apply to the extent that such particular statements are made known to other public authorities or other agencies for public administration purposes unless the law forbids it.
(2a) Subsections (1) and (2) above shall apply mutatis mutandis when a data protection officer without authorisation discloses the secret of another within the meaning of these provisions, which was entrusted to or otherwise revealed to one of the persons named in subsections (1) or (2) above in their professional capacity and of which he has gained knowledge in the course of the fulfilment of his duties as data protection officer.
(3) Other members of a bar association shall be deemed to be equivalent to an attorney named in subsection (1) No 3 above. The persons named in subsection (1) and the 1st sentence above shall be equivalent to their professionally active assistants and those persons who work with them in training for the exercise of their profession. After the death of the person obliged to keep the secret, whosoever acquired the secret from the deceased or from his estate shall be equivalent to the persons named in subsection (1) and in the 1st and 2nd sentences above.
(4) Subsections (1) to (3) above shall also apply if the offender unlawfully discloses the secret of another person after the death of that person.
(5) If the offender acts for material gain or with the intent of enriching himself or another or of harming another the penalty shall be imprisonment not exceeding two years or a fine.

fined as facts that only certain people know about and have a special interest in their confidentiality.[112]

iii. Does your country's penal law allow or even require clinicians, lawyers, priests, etc. to breach the confidentiality in certain situations or for certain reasons established by law? Under which standards would that be done? (e.g. reasonable cause to believe that there is abuse vs. seeing an abused child, women, elderly)?

Sec. 203 PC criminalizes the disclosure of secrets only in case it is not authorized by law. An authorized disclosure on the other hand is lawful. It is not clear under German law if an authorized disclosure does not fall within the purview of sec. 203 PC at all or if the authorization only lends a justification – or if both is true to a certain degree[113].

A disclosure of secrets is not unlawful in the following cases:

- **Consent of the secret's subject**
- **Other justifications, e.g. necessity**

In case the carrier of a secret is obliged to give evidence concerning certain circumstances, the disclosure of secrets is justified. If the person has a right to silence (sec. 53, 53a Code of Criminal Procedure, 383 Code of Civil Procedure), a justification of the disclosure of secrets can only be derived from the general rules of necessity in sec. 34 PC[114] if the interest in establishing the truth is of higher value than the interest of the secret's subject in its confidentiality. This can be true if the disclosure serves the prevention of an imminent danger[115].

- **Legal obligation to disclose information**

If the law establishes a duty to disclose personal information, the law values the public interest in the disclosure higher than the person's interest in the secrecy of information. Such obligations to disclose information are legally established for example for medical practitioners:

- Concerning certain illnesses that are to be indicated to public health service agencies;
- Obligations to indicate occupational diseases to statutory accident insurance institutions;

[112] Entscheidungen des Bundesgerichtshofs in Strafsachen (hereinafter: "BGHSt") 41, 140, 142.
[113] Vgl. S/S-*Lenckner*, § 203 marginal no. 21.
[114] **Section 34 PC: Necessity**
A person who, faced with an imminent danger to life, limb, freedom, honour, property or another legal interest which cannot otherwise be averted, commits an act to avert the danger from himself or another, does not act unlawfully, if, upon weighing the con icting interests, in particular the affected legal interests and the degree of the danger facing them, the protected interest substantially outweighs the one interfered with. This shall apply only if and to the extent that the act committed is an adequate means to avert the danger.
[115] LK-*Schünemann*, § 203 marginal no. 132 ff.

- Obligations to indicate the prescription of substances substituting illegal drugs;
- Obligations to inform statutory health insurance agencies;
- Obligations to inform public registration offices about birth or death of citizens.

Sec. 138 PC[116] establishes a duty to disclose information about planned severe crimes for everyone.

Apart from this, specific information can lawfully be disclosed by public authorities in order to protect people's interest, for example medical personnel or state-recognized social workers can inform youth welfare services of specific threats children may face in difficult family circumstances.

b. Subject – Type of perpetrators?

Does the criminal law of your country identify the categories of professionals who are bound by specific confidentiality rules?

Yes, sec. 203 PC enumerates exclusively professionals who bear certain obligations to confidentiality concerning personal secrets:

In subsection 1:

[116] **Section 138 PC: Omission to bring planned offences to the attention of the authorities**
(1) Whosoever has credible information about the planning or the commission of the following offences:
1. preparation of a war of aggression (section 80);
2. high treason under sections 81 to 83 (1);
3. treason or an endangerment of peace under sections 94 to 96, section 97a or section 100;
4. counterfeiting money or securities under section 146, section 151, section 152 or counterfeiting debit cards and blank euro cheque forms under section 152b (1) to (3);
5. murder under specific aggravating circumstances (section 211), murder (section 212), genocide (section 6 of the Code of International Criminal Law), a crime against humanity (section 7 of the Code of International Criminal Law), or a war crime (section 8, section 9, section 10, section 11 or section 12 of the Code of International Criminal Law);
6. an offence against personal liberty in cases under section 232 (3), (4), or (5), section 233 (3), each to the extent it involves a felony, section 234, section 234a, section 239a or section 239b;
7. robbery or blackmail using force or threat to life and limb (sections 249 to 251 or section 255); or
8. offences creating a danger to the public under sections 306 to 306c, section 307 (1)to (3), section 308 (1) to (4), section 309 (1) to (5), section 310, section 313, section 314, section 315 (3), section 315b (3), section 316a or section 316c at a time when the commission or result can still be averted, and fails to report it in time to the public authorities or the person threatened, shall be liable to imprisonment not exceeding five years or a fine.
(2) Whosoever credibly learns
1. of the commission of an offence under section 89a or
2. of the planning or commission of an offence under section 129a, also in conjunction with section 129b (1), 1st and 2nd sentences, at a time when the commission can still be averted, and fails to report it promptly to the public authorities, shall incur the same penalty. Section 129b (1) 3rd to 5th sentences shall apply mutatis mutandis in the case of No. 2 above.
(3) Whosoever by gross negligence fails to make a report although he has credible information about the planning or the commission of an unlawful act, shall be liable to imprisonment of not more than one year or a fine.

“1. physician, dentist, veterinarian, pharmacist or member of another healthcare profession which requires state-regulated education for engaging in the profession or to use the professional title;

2. professional psychologist with a final scientific examination recognized by the State;

3. attorney, patent attorney, notary, defence counsel in statutorily regulated proceedings, certified public ac-countant, sworn auditor, tax consultant, tax agent, or organ or member of an organ of a law, patent law, accounting, auditing or tax consulting firm in the form of a company;

4. marriage, family, education or youth counsellor as well as addiction counsellor at a counselling agency which is recognised by a public authority or body, institution or foundation under public law;

4a. member or agent of a counselling agency recognised under section 3 and section 8 of the Act on Pregnan-cies in Conflict Situations;

5. a state-recognised social worker or state-recognised social education worker; or

6. member of a private health, accident or life insurance company or a private medical, tax consultant or attorney invoicing service.”

In subsection 2:

“1. public official;

2. person entrusted with special public service functions;

3. person who exercises duties or powers under the law on staff employment representation;

4. member of an investigative committee working for a legislative body of the Federation or a state, another committee or council which is not itself part of the legislative body, or as an assistant for such a committee or council;

5. publicly appointed expert who is formally obliged by law to conscientiously fulfil his duties, or

6. person who is formally obliged by law to conscientiously fulfil his duty of confidentiality in the course of scientific research projects”

In subsection 2a:

“Subsections (1) and (2) above shall apply mutatis mutandis when a data protection officer without authorisation discloses the secret of another within the meaning of these provisions, which was entrusted to or otherwise revealed to one of the persons named in subsections (1) or (2) above in their professional capacity and of which he has gained knowledge in the course of the fulfilment of his duties as data protection officer”

In subsection 3:

"The persons named in subsection (1) and the 1st sentence above shall be equivalent to their professionally active assistants and those persons who work with them in training for the exercise of their profession. After the death of the person obliged to keep the secret, whosoever acquired the secret from the deceased or from his estate shall be equivalent to the persons named in subsection (1) and in the 1st and 2nd sentences above."

This regulation shall hinder the avoidance of the prohibition by disclosing secrets through actions of staff members.

c. Act – illegal use and transfer/distribution?

Which acts (e.g. illegal collection, use, transfer and distribution) are specifically penalized by your country's criminal law?

Sec. 203 PC criminalizes the disclosure of personal secrets. Disclosure is defined as giving notice of confident information to persons who formerly did not know about the disclosed information.[117]

Moreover sec. 204 criminalizes the exploitation of other person's personal secrets[118]. Exploitation is defined as the gaining of financial benefits by making use of certain information without disclosing it to others[119]. The elements of the offence description are for example met if a patent attorney uses a client's invention for his own financial benefit[120].

Besides, the illegal collection or use of data is sanctioned by the regulations mentioned above (C) (b) 1. b. and also (C) (b) 3. c.

Apart from this sec. 201 ss. PC apply:

Section 201: Violation of the privacy of the spoken word

Section 201a: Violation of intimate privacy by taking photographs

Section 202: Violation of the privacy of the written word

Section 202a: Data espionage

Section 202b: Phishing

Section 202c: Acts preparatory to data espionage and phishing

[117] Entscheidungen des Reichsgerichts in Strafsache RGSt 26, 5; 38, 62; BGHSt 27, 120, 121; BGH Neue Juristische Wochenschrift 1995, 2915.

[118] **Section 204 PC: Exploitation of the secrets of another**
(1) Whosoever unlawfully exploits the secret of another, in particular a business or trade secret, which he is obliged to keep secret pursuant to section 203, shall be liable to imprisonment not exceeding two years or a fine.

[119] *Fischer*, § 204 marginal no. 3.

[120] *Fischer*, § 204 marginal no. 3; S/S-*Lenckner*, § 204 marginal no. 5.

Section 355: Violation of the tax secret

3. Illegal processing of personal and private data

a. Object?

Does your criminal law penalize the illegal and unauthorized acquisition, processing, storage, analysis, manipulation, use, sale, transfer etc. of personal and private data?

Yes, see (C)(b) 1. b.ii.

b. Subject?

Does your criminal law identify specifically the categories of persons and entities included in this criminal prohibition and sanctions?

As far as specific regulations pertaining to certain areas do exist, the categories of persons and entities that are addressed by these regulations are identified in the regulations themselves.

If the general rules of the Federal Data Protection Act are admissible, there is no restriction to a certain group of persons or entities. Hence the regulations of the Federal Data Protection Act apply to public as well as to private persons or entities, sec. 1 Federal Data Protection Act.[121]

[121] **Sec. 1 Federal Data Protection Act: Purpose and scope**
(1) The purpose of this Act is to protect individuals against infringement of their right to privacy as the result of the handling of their personal data.
(2) This Act shall apply to the collection, processing and use of personal data by
1. public bodies of the Federation,
2. public bodies of the Länder, where data protection is not covered by Land legislation and where the Länder
a) execute federal law, or
b) act as judiciary bodies and administrative matters are not involved,
3. private bodies that collect data for use in data processing systems, or use such systems to process or use data, or collect data in or from non-automated filing systems, or use such systems to process or use data, unless the data are collected, processed or used solely for personal or domestic activities.
See also: **Sec. 2 Federal Data Protection Act: Public and private bodies**
(1) "Public bodies of the Federation" shall mean the authorities, judiciary bodies and other public-law institutions of the Federation, of the direct federal corporations, institutions and foundations under public law as well as their associations irrespective of their legal forms. The successor companies created by law from the Special Fund "Deutsche Bundespost" shall be considered public bodies as long as they have an exclusive right under the Postal Act.
(2) "Public bodies of the Länder" shall mean the authorities, judiciary bodies and other public-law institutions of a Land, of a municipality, an association of municipalities or other legal persons under public law subject to Land supervision as well as their associations irrespective of their legal forms.
(3) Private-law associations of public bodies of the Federation and the Länder performing public administration tasks shall be considered public bodies of the Federation irrespective of private shareholdings if
1. they operate in more than one Land, or
2. the Federation possesses the absolute majority of shares or votes.
Otherwise, they shall be regarded as public bodies of the Länder.

c. Act?

i. Does your criminal law penalize specific acts that constitute all or part of the illegal processing of personal and private data? Reply for each category listed below citing the relevant law and its provisions, if available:

1. Illegal collection

Yes, see:

Section 43 Federal Data Protection Act: Administrative offences
… (2) An administrative offence shall be deemed to have been committed by anyone who, whether intentionally or through negligence
1. collects or processes personal data which are not generally accessible without authorization,
2. makes available personal data which are not generally accessible by means of automated retrieval without authorization,
3. retrieves personal data which are not generally accessible without authorization, or obtains such data for themselves or others from automated processing operations or non-automated files without authorization,
4. obtains transfer of personal data which are not generally accessible by providing false information,
5. in violation of Section 16 (4) first sentence, Section 28 (5) first sentence, also in conjunction with Section 29 (4), Section 39 (1) first sentence or Section 40 (1), uses transferred data for other purposes,
5 a. in violation of Section 28 (3b) makes the conclusion of a contract dependent on the consent of the data subject,
5 b. in violation of Section 28 (4) first sentence processes or uses data for purposes of advertising or market or opinion research,
6. in violation of Section 30 (1) second sentence, Section 30a (3) third sentence or Section 40 (2) third sentence combines a feature referred to there with specific information, or
7. in violation of Section 42a first sentence, fails to notify or fails to do so correctly, completely or within the prescribed time limit.

Section 44 Federal Data Protection Act: Criminal offences
(1) Anyone who wilfully commits an offence described in Section 43 (2) in exchange for payment or with the intention of enriching him-/herself or another person, or of harming another person shall be liable to imprisonment for up to two years or to a fine.

Apart from these specific regulations further provisions with the same content exist in certain areas as for example in the Telecommunications Act.

2. Illegal use

The illegal use of personal data is not generally criminalized in the Federal Data Protection Act. Yet, in case the use of data is administered in a certain situation or context, special regulations apply. The legislator refused to create a general provision on the illegal use of data in

(4) "Private bodies" shall mean natural or legal persons, companies and other private-law associations not covered by subsections 1 through 3. If a private body performs sovereign public administration tasks, it shall be a public body within the meaning of this Act.

order to avoid this regulation from admission in cases of a use of data which affect the data subject's interests insignificantly. The legislator took the view that it was disproportionate to establish an administrative offence covering such situations. Thus the illegal use of personal data is sanctioned only by sec. 43 subsec. 2, no. 5, 5b Federal Data Protection Act[122] – that is if the perpetrator uses data for a different purpose than the one the data was meant to serve or if the perpetrator ignores an objection of the data subject to the collection or use of the data. If the perpetrator commits the offence aiming at financial interests, his behaviour amounts to a criminal offence.

Special provisions concerning for example the field of telecommunications services apply as well.

3. Illegal retention

The illegal retention of data is covered by the offence description of sec. 43 subsec. 2 no. 1 Federal Data Protection Act[123]. There the unlawful processing of data is sanctioned. Sec. 43 subsec. 2 no. 5b applies to the unlawful retention of data for purposes of advertising or opinion research as well.

Processing is defined as „recording, alteration, transfer, blocking and erasure of personal data", sec. 3 subsec. 4 Federal Data Protection Act. Again, if the prerequisites of sec. 44 Federal Data Protection Act are met, the behaviour amounts to a criminal offence.

Special provisions concerning for example the field of telecommunications services apply as well.

4. Illegal transfer

Illegal transfer is criminalized as mentioned in (C)(b) 3.c.3.

ii. Does it make a difference if these personal and private data are used, transferred etc. for police or law enforcement purposes?

[122] Sec. 43 Federal Data Protection Act: Administrative Offences
(2) An administrative offence shall be deemed to have been committed by anyone who, whether intentionally or through negligence
5. in violation of Section 16 (4) first sentence, Section 28 (5) first sentence, also in conjunction with Section 29 (4), Section 39 (1) first sentence or Section 40 (1), **uses** transferred data for other purposes,
5 b. in violation of Section 28 (4) first sentence **processes** or **uses** data for purposes of advertising or market or opinion research,

[123] (2) An administrative offence shall be deemed to have been committed by anyone who, whether intentionally or through negligence
1. collects or processes personal data which are not generally accessible without authorization, …

The collection, processing or use of data is generally ruled by sec. 4 subsec. 1 Federal Data Protection Act. This regulation applies for police or law enforcement agencies as well. Data collection by law enforcement authorities is lawful only if special legal provisions allow for it.

d. Justification?

i. Under which conditions does your country's law allow for the authorized collection, processing, transfer and distribution of personal and private data?

See (C)(b)1.c.i.

ii. What standard of need is required for an authorized collection and/or distribution of personal and private data (compelling, important, reasonable, convenient)?

See (C)(b)1.c.ii.

4. Identity theft

(Note: identity theft occurs when someone appropriates another's personal information without his or her knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating fraud schemes. Typically, the victim is led to believe they are divulging sensitive personal information to a legitimate business or entity, sometimes as a response to an e-mail solicitation to update billing or membership information, or as an application for a fraudulent Internet job posting or loan.)

a. Object

i. Does your criminal law penalize identity theft? Please, cite the relevant law.

The German data protection law does not contain a special regulation on identity theft. However, specific actions concerning identity theft can be criminalized as administrative or criminal offences. This is true for certain preparatory offences, for offences of unlawful collection as well as processing and use of unlawfully obtained data. Due to the existing wide spread regulations on unlawful data collection and use, the legislator felt it not necessary to establish a special offence of identity theft. Moreover, this is the reason that there does not exist a specific regulation on „phishing" in the German law on data protection.

The use of data usually amounts to an offence of computer fraud, sec. 263a PC, as well as data espionage, sec. 202a PC.

As for the collection of data, the admissibility of criminal offences is contentious.

The collecting of data by use of Trojans or keyloggers is an offence under sec. 202a PC. Besides, this usually amounts to offences under sec. 303a and sec. 303b PC. Man-in-the-middle-attacks are criminalized by sec. 202b PC. If the perpetrator gains data by the victim's response

to phishing-mail or fraudulent websites, neither the offence description of sec. 202a nor of sec. 202b is met. Still, the creation of the phishing mail as well as of fraudulent websites is criminalized by sec. 269 PC.[124]

Irrespective of the way the data is being collected, sec. 43, 44 Federal Data Protection Act criminalize the fact that data is being collected without the data subject's consent.

The question as to whether apart from this fraud under section 263 PC can already be committed by the collection of data is debated heavily[125]. The admissibility of sec. 263 PC presupposes that the mere collection of data damaged the victim's financial interests. Some authors think that this cannot be held true. In their view, a damage of the victim's financial interests presupposes further actions of the perpetrator.

By establishing sec. 202c PC in the year 2007 the German legislator criminalized (without even realizing at that time) the „phishing" of data and thereby identity theft. Only very few actions remain beyond the ambit of the offence description of 202c PC – for example the sending of phishing mails without receiving any response.

However, when it comes to phishing, sec. 202c PC does not bear great importance, for the offences of illegal data collection and usage take precedence over sec. 202c PC.

ii. Does your criminal law proscribe specific forms of identity theft, like phishing, for example? Phishing is defined as a form of online identity theft that uses spoofed emails designed to lure recipient to fraudulent websites which attempt to trick them into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc.

See (C)(b)4.a.i.

b. Subject

Does your criminal law contain penal responsibility connected to a person's digital personality, or to his/her Avatar, or to his/her digital role in an internet based simulation game (e.g. Cityville, Farmville, etc.)? Please cite the relevant law.

No, a specific provision criminalizing a person's behaviour under his/her Avatar's role does not exist. Actions can only be criminalized if they amount to an action of a natural person.

[124] **Section 269 PC: Forgery of data intended to provide proof**
(1) Whosoever for the purposes of deception in legal commerce stores or modifies data intended to provide proof in such a way that a counterfeit or falsified document would be created upon their retrieval, or uses data stored or modified in such a manner, shall be liable to imprisonment not exceeding five years or a fine. …

[125] In favor of punishment under sec. 263 PC: *Weber,* HRRS 2004, 406, 409; *Hilgendorf/Frank/Valerius,* Computer- und Internetstrafrecht, Rn. 765; against punishment under sec. 263: *Graf,* Neue Zeitschrift für Strafrecht 2007, 129, 130.

(c) Protection Against Illegal Content: ICT Related

1. Object

a. Child pornography - images of real or virtual children?

i. Does your penal law criminalize the use of the internet for the purpose of storing, accessing, and disseminating child pornography? If so, please, cite the relevant law.

The dissemination of child pornography by use of the internet is criminalized in sec. 184 b subsec. 1 no.1, 2 PC.[126] Access and possession of child pornography material are also criminalized, sec. 184b subsec. 4 PC.[127]

The offence of illegal storage of child pornography material does not only apply for the storage on a hard disc but as well for the storage as virtual memory (though this view is challenged by some authors).[128] Sec. 184d PC[129] criminalizes furthermore the broadcasting of child pornographic actions. Several provisions concerning the prohibition of child pornography are to be found in the German law on Youth Protection.

ii. In particular, does your criminal law:
Create a new offense that targets criminals who use the Internet to lure and exploit children for sexual purposes? Make it a crime:
1. to transmit,
2. make available,
3. export

[126] **Section 184b PC: Distribution, acquisition and possession of child pornography**
(1) Whosoever
1. disseminates;
2. publicly displays, presents, or otherwise makes accessible; or
3. produces, obtains, supplies, stocks, offers, announces, commends, or undertakes to import or export in order to use them or copies made from them within the meaning of Nos 1 or 2 above or facilitates such use by another pornographic written materials (section 11 (3)) related to sexual activities performed by, on or in the presence of children (section 176 (1)) (child pornography)
shall be liable to imprisonment from three months to five years.
(2) Whosoever undertakes to obtain possession for another of child pornography reproducing an actual or realistic activity shall incur the same penalty.
(3) In cases under subsection (1) or subsection (2) above the penalty shall be imprisonment of six months to ten years if the offender acts on a commercial basis or as a member of a gang whose purpose is the continued commission of such offences and the child pornography reproduces an actual or realistic activity.

[127] **Sec. 184b PC: Distribution, acquisition and possession of child pornography**
(4) Whosoever undertakes to obtain possession of child pornography reproducing an actual or realistic activity shall be liable to imprisonment not exceeding two years or a fine. Whosoever possesses the written materials set forth in the 1st sentence shall incur the same penalty.

[128] *Fischer*, § 184b marginal no. 20; *Marberth-Kubicki*, marginal no. 225 ss.

[129] **Section 184d PC: Distribution of pornographic performances by broadcasting, media services or telecommunications services**
Whosoever disseminates pornographic performances via broadcast, media services, or telecommunications services shall be liable pursuant to sections 184 to 184c. In cases under section 184 (1) the 1st sentence above shall not apply to dissemination via media services or telecommunications services if it is ensured by technical or other measures that the pornographic performance is not accessible to persons under eighteen years of age.

4. and intentionally access child pornography on the Internet;

Sec. 176 subsec. 4 no. 3 PC[130] (see (C) (c) 1. a. iii.) criminalizes the contacting of children by use of the internet for purposes of a future child abuse in the real world, so-called „cyber-grooming". The transmission/making accessible/accessing of child pornography material is not criminalized explicitly in sec. 176 subsec. 3 PC. However, the provision criminalizes the inducing of a child by presenting it with pornographic material.

The transmission/making accessible/accessing of child pornography material is criminalized by sec. 184 ss. PC. Those provisions do not presuppose a certain purpose of preparing future child abuse offences in the real world like „cyber-grooming".

ii. In particular, does your criminal law: Allow judges to order the deletion of child pornography posted on computer systems in your country;

There has been a controversial discussion in Germany as to whether the constitution allows for a censoring of child pornographic contents that are disseminated by use of the internet.[131]

In the year 2009 a statute was adopted that obliged internet providers to block websites displaying child pornographic content. Yet the political parties were discussing whether the blocking of internet sites was the best thing to do. They concluded that it would be much better to directly erase child pornographic contents rather than to just block them. So the mentioned law was never enforced. Finally, it was repealed in the year 2011[132].

Nowadays child pornographic contents are directly erased by internet providers. Companies active in the internet sector cooperate with the Federal Police Agency in order to make sure that no child pornographic contents are available on the internet. The international network INHOPE (International Association of Internet Hotlines) cooperates with national authorities and internet businesses in order to combat child pornography on the internet. If child pornographic contents are detected by one of the network members, the national INHOPE-partners are contacted[133]. The responsible host-provider is requested to erase the content. Since in Europe the refusal to erase illegal content amounts to a criminal offence[134], at least European

[130] **Section 176 PC: Child abuse**
(4) Whosoever
… 3. presents a child with written materials (section 11(3)) to induce him to engage in sexual activity with or in the presence of the offender or a third person or allow the offender or a third person to engage in sexual activity with him; … shall be liable to imprisonment from three months to five years.

[131] *Gercke*, ZUM 2011, 625; *Heliosch*, Verfassungsrechtliche Anforderungen an Sperrmaßnahmen von kinderpornographischen Inhalten im Internet, p. 249 ss.; *Koreng*, Zensur im Internet, p. 120; *Schnabel*, Juristenzeitung 2009, 996; *Sieber*, Juristenzeitung 2009, 653.

[132] 2011 Federal Law Gazette I, p. 2958.

[133] See INHOPE Annual Report 2011.

[134] *Sieber*, Straftaten und Strafverfolgung im Internet, Gutachten zum 69. Deutschen Juristentag, C 60 ff.

providers are naturally interested to erase the contents immediately[135]. Thus the efforts to erase child pronography are rather successful – two weeks after the first notification 90% of the sites are usually erased, after four weeks usually 98% of the contents are erased[136].

ii. In particular, does your criminal law: Allow a judge to order the forfeiture of any materials or equipment used in the commission of a child pornography offense;

Yes, German courts can order the forfeiture of materials that were used in the commission of child pornography offences. This is true for any type of data medium (e.g. hard disk, floppy disk, CD, DVD, Mini-Disk, cassette) – as far as materials of child pornography are stored thereon, sec. 74d PC[137]. The order of forfeiture is mandatory for written documents as well as other data storage materials containing child pornography materials that were designed for dissemination or making accessible for the public.

As far as offences under sec. 184b subsec. 2, 4 PC are concerned, the specific provision of sec.184b subsec. 6 PC[138] rules that objects to which an offence under sec. 184b PC relates are subject to a deprivation order[139]. This specific provision was necessary because in many cases the perpetrator in possession of child pornography material does not want to disseminate the

[135] *Sieber*, Straftaten und Strafverfolgung im Internet, Gutachten zum 69. Deutschen Juristentag, C 139.
[136] BT-Drucks. 17/6644, p. 6.
[137] **Section 74d PC: Deprivation and destruction of publication media**
(1) Written materials (section 11(3)) of a content every intentional dissemination of which with knowledge of the content would fulfil the elements of a criminal provision, shall be subject to a deprivation order if at least one copy was disseminated through an unlawful act or was intended for such dissemination. At the same time the equipment used for or intended for the production of the written material, such as plates, frames, type, blocks, negatives or stencils, shall be destroyed.
(2) The deprivation shall extend only to those copies which are in the possession of the persons involved in their dissemination or preparation or which have been publicly displayed or, if they were sent for dissemination, have not yet been distributed to the recipient.
(3) Subsection (1) above shall apply mutatis mutandis to written materials (section 11(3)) of a content the intentional dissemination of which with knowledge of the content would fulfil the elements of a criminal provision only under additional circumstances. Deprivation and destruction shall not be ordered unless 1. the copies and the objects indicated in subsection (1) 2nd sentence above are in the possession of the principal or secondary participant or another on whose behalf the principal or secondary participant acted, or are intended by these people for dissemination; and 2. the measures are required to prevent any unlawful dissemination by these persons.
(4) Dissemination within the meaning of subsections (1) to (3) above shall also mean providing access to written material (section 11(3)) or at least one copy of it to the public by putting it on display, putting up posters, performances or other means.
(5) Section 74b(2) and (3) shall apply mutatis mutandis.
[138] **Sec. 184b PC**
(6) In cases under subsection (3) above section 73d shall apply. Objects to which an offence under subsection (2) or (4) above relates shall be subject to a deprivation order. Section 74a shall apply.
[139] **Section 184b PC: Distribution, acquisition and possession of child pornography**
(2) Whosoever undertakes to obtain possession for another of child pornography reproducing an actual or realistic activity shall incur the same penalty.
(4) Whosoever undertakes to obtain possession of child pornography reproducing an actual or realistic activity shall be liable to imprisonment not exceeding two years or a fine. Whosoever possesses the written materials set forth in the 1st sentence shall incur the same penalty.

material or to make it accessible to the public[140]. Sec. 184c subsec. 5 PC rules that sec. 184b subsec. 6 applies accordingly to youth pornography materials.

ii. In particular, does your criminal law criminalize 1. Knowingly accessing child pornography on the internet

Yes, this behaviour is criminalized in sec. 184b subsec. 4 PC:

(4) Whosoever undertakes to obtain possession of child pornography reproducing an actual or realistic activity shall be liable to imprisonment not exceeding one year or a fine. The 1st sentence shall not apply to acts of persons related to juvenile pornography produced by them while under eighteen years of age and with the consent of the persons therein depicted.
It is also punishable under sec. 184b subsec. 2 PC to obtain possession of child pornography for another:
(2) Whosoever undertakes to obtain possession for another of juvernile pornography reproducing an actual or realistic activity shall incur the same penalty.

The offence description is met if a person downloads child pornography from the internet and stores the material on data media (e.g. hard disk, floppy disk, CD, DVD, Mini-Disk, cassette).

It is not clear whether the mere storage in the main or cache memory fulfills the prerequisites of the offence description. If this was true, then the mere observing of child pornography would already amount to the offence of obtaining possession of child pornography – as observed material is stored automatically at least in the cache memory of the used computer. Yet in most of those cases the person looking at pornography will not intent – let alone even know about – the storage of this data on his computer. In the end, the intention of the consumer of child pornography will depend upon his technical knowledge.

ii. In particular, does your criminal law criminalize 2. Transmitting child pornography on the internet

The term „transmission of child pronography“ is not used in the German Criminal Law. However, sec. 184b subsec. 1 no. 1, 2, 184d subsec. 1PC criminalize the dissemination and making accessible of child pornography.

Dissemination (sec. 184b subsec. 1 no. 1 PC[141])

In earlier times dissememination was interpreted as physical handover from hand to hand[142]. Since this interpretation would not encompass the transmission of stored data, the Federal

[140] BT-Drucks. 12/3001, p. 4.
[141] See footnote 139.
[142] BGHSt 47, 55, 59; BGH Neue Juristische Wochenschrift 2005, 689, 690; S/S-*Perron/Eisele*, § 184b marginal no. 5.

Criminal Court created a new definition of dissemination encompassing the dissemination by use of the internet in the year 2001[143]. A dissemination by use of the internet is committed if data has reached the recipient's computer – for example the virtual memory. It is irrelevant whether this is realized by a user's download or by a provider's upload.

Making accessible (sec. 184b subsec. 1 no. 2 PC[144]) presupposes that the data is posted on the internet and made available for others[145].

Dissemination as well as **making accessible** is committed only if the data are available for a considerable number of persons – it does not suffice that only one or few people receive the data[146]. Yet, this would amount to an offence under sec. 184b subsec 2, subec. 1 no. 3 or sec. 184 subsec. 1 no. 1 PC.

ii. In particular, does your criminal law criminalize
3. Exporting child pornography on the internet

Sec. 184b subsec. 1 no. 3 PC criminalizes preparatory acts to the offences under sec. 184b I no. 1 and 2 PC. This encompasses the undertaking of an exportation of child pornography with the aim to disseminate or make it available to others (as for this purpose see (C) (c) 1. a. ii. 3.1.). Again, the material has to be made accessible to a considerable number of persons – it does not suffice if the material is available only for few people.

Exportation is defined as the transfer beyond the borders of Germany.[147] It encompasses the electronic transmission to foreign countries by use of the internet.[148]

ii. In particular, does your criminal law criminalize
4. Possessing child pornography on the internet for the purpose of, e.g., transmitting, exporting it…?

Sec. 184b subsec. 1 no. 3 PC criminalizes the storage of child pornography with a purpose to disseminate (parts of) or make it accessible to others. The same is true for youth pornography, sec. 27 subsec. 1 no. 2, 15 subse. 1 no. 7, subsec. 2 no. 1 Youth Protection Act.

The offence description encompasses the storage of child pornography on the hard disc[149]. The ambit of sec. 184d subsec. 1 PC does not extend to transmitted "live-acts" that can be watched but not stored[150].

[143] BGHSt 47, 55, 60.
[144] See footnote 139
[145] BGHSt 47, 55, 60 f.
[146] Münchener Kommentar PC-*Hörnle* (hereinafter: „MüKo-author"*)*, § 184b marginal no. 18.
[147] MüKo-*Hörnle*, § 184b marginal no. 24, § 184 marginal no. 97.
[148] MüKo-*Hörnle*, § 184b marginal no. 24, § 184, marginal no. 97.
[149] MüKo-*Hörnle*, § 184b marginal no. 25; *König*, Kinderpornografie im Internet, marginal no. 239.
[150] *Fischer*, § 184d marginal no. 6.

As for the possession of child pornographic written documents under sec. 184b subsec. 4 PC, this does not presuppose one of the aims mentioned in sec. 184b subsec. 1 no. 3 PC see. (C) (c) 1. a. ii. 3. 1.

iii. Does your criminal law penalize the online solicitation of children for sexual purposes via social networking websites and chat rooms?

Cyber-grooming is criminalized in sec. 176 subsec. 4 no. 3 PC[151]. It is punishable under sec. 176 subsec. 4 no. 3 PC to present a child with written material to induce sexual activity.

The introduction of this provision into the Penal Code was the legislator's reaction to press reports on adults contacting children for sexual purposes by use of the internet[152]. This had not been punishable before since it was deemed a mere preparatory act to child abuse under sec. 176, 176a PC[153]. The loophole was closed by the introduction of the preparatory offence. The provision is criticized as producing conflicts: Only the influencing of children by use of written material is criminalized in the provision but not the inducing by presents or other means. Moreover the preparation of sexual offences is now criminalized whereas the preparation of other capital crimes like for example murder by a sole perpetrator is not being criminalized under German criminal law[154].

The inducing of children is defined as immediate psychological influence of considerable persistency[155]. The influencing need not be explicitly sexual related[156]. The crucial element is the perpetrator's aim to induce the child to engage in sexual activity.

The offence description is met for example if a child is influenced by promises, persuasion or exercising of pressure[157]. This can be realized in chat-rooms as well as by web-cam-transmission or by use of social networks. Special consideration has to be dedicated to the

[151] **Section 176 PC: Child abuse**
(4) Whosoever
1. engages in sexual activity in the presence of a child;
2. induces the child to engage in sexual activity, unless the act is punishable under subsection (1) or subsection (2) above;
3. presents a child with written materials (section 11(3)) to induce him to engage in sexual activity with or in the presence of the offender or a third person or allow the offender or a third person to engage in sexual activity with him; or
4. presents a child with pornographic illustrations or images, audio recording media with pornographic content or pornographic speech,
shall be liable to imprisonment from three months to five years.
(5) Whosoever supplies or promises to supply a child for an offence under subsections (1) to (4) above or who agrees with another to commit such an offence shall be liable to imprisonment from three months to five years.
[152] BT-Drucks. 15/350, p. 17 s.
[153] BT-Drucks. 15/350, p. 18.
[154] *Duttge/Hörnle/Renzikowski*, Neue Juristische Wochenschrift 2004, 1065, 1067 f.; *Lackner/Kühl*, § 176 marginal no. 4a; S/S-*Perron/Eisele*, § 176 marginal no. 14.
[155] BT-Drucks. 15/350, p. 18; BGH Neue Zeitschrift für Strafrecht 2011, 455.
[156] *Fischer*, § 176 marginal no. 14; MüKo-*Renzikowski*, § 176 marginal no. 38.
[157] BGHSt 45, 158, 161; MüKo-*Renzikowski*, § 176 marginal no. 38.

prerequisite of persistence. Usually it will not suffice if the perpetrator contacts a child only once or in a rather retentive way.[158]

Written materials are defined in sec. 11 subsec. 3 PC[159]. The provision rules that the term „written material" comprises audiovisual media and other data storage media. The prevalent view in German doctrine suggests that this encompasses even the computer's virtual memory.[160] Accordingly already the transmission of messages amounts to an offence under sec. 176 PC since the data are stored in the virtual memory of the receiver's computer as soon as he downloads the message.

As for „real time chats" and „streamings" the element of storage is not fulfilled – therefore these actions do not amount to an offence under sec. 176 subsec. 4 no. 3 PC[161].

iv. Is the definition of child pornography in your criminal code close to that contained in international instruments (e.g. EU Directives)?

The term child pornography is not defined in the German criminal code. Yet the term pornographic written material is defined in sec. 184b subsec. 1 PC[162] as material related to sexual activities performed by, on or in the presence of children.

According to sec. 184g no. 1 PC[163] sexual activities shall only be those which are of some relevance to the protected legal interests. Sexual activities in presence of others shall only relate to activities that are really observed by others.

Children are persons under 14 years of age, sec. 176 subsec. 1 PC. Written materials containing sexual activities by, on or in presence of persons between the ages of fourteen to eighteen years are defined as juvenile pornography.

The term written material encompasses audiovisual media and data storage media, sec. 11 subsec. 3 PC (see (C) (c) 1. a. iii.). „Live performances" that cannot be defined as written material fall within the purview of sec. 184d PC[164].

---

[158] So auch *Hube*, Kriminalistik 2011, 71, 72; LK-*Hörnle*, § 176, Rn. 88.

[159] **Sec. 11 subsec. 3 PC: Definitions**
(3) Audiovisual media, data storage media, illustrations and other depictions shall be equivalent to written material in the provisions which refer to this subsection.

[160] *Fischer*, § 184b marginal no. 20; *Marberth-Kubicki*, Rn. 225 ff.

[161] *Frühsorger*, Der Straftatbestand des sexuellen Kindesmissbrauchs gemäß § 176 StGB, p. 139; *Hilgendorf/Frank/Valerius,* Computer- und Internetstrafrecht, marginal no. 272; LK-*Hörnle*, § 176 marginal no. 90.

[162] **Section 184b PC Distribution, acquisition and possession of child pornography**
(1) ... pornographic written materials (section 11 (3)) related to sexual activities performed by, on or in the presence of children (section 176 (1)) (child pornography).
shall be liable to imprisonment from three months to five years

[163] **Section 184g PC: Definitions**
Within the meaning of this law 1. sexual acts and activities shall only be those which are of some relevance in relation to the protected legal interest in question;
2. sexual acts and activities in the presence of another shall be those which are committed in the presence of another who observes them.

Not yet answered is the question as to when the threshold to child pornographic content is passed. The legislator left the answer to this question to judicial practice.

This has led to a definition that describes pornographic content as display of sexual activities in an overly crude manner and at the expense of human interaction and activity. The portrayal of sexual activities is entirely or primarily concerned with sexual stimulation[165]. Since the creation of this definition in the late 1960s[166] there has been contention on the correct definition of pornography in legal doctrine[167]. In legal literature very often a definition of pornography as display of sexual activity disregarding the dignity of the human being and making him or her subject to sexual desires of others is suggested.

Art. 2 lit.c of the Directive 2011/92/EU of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pronography (replacing Council Framework Decision 2004/68/JHA) defines **child pornography** as

(i) any material that visually depicts a child engaged in real or simulated sexually explicit conduct;
(ii) any depiction of the sexual organs of a child for primarily sexual purposes;
(iii) any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes; or
(iv) realistic images of a child engaged in sexually explicit conduct or realistic images of the sexual organs of a child, for primarily sexual purposes;

Art. 9 subsec. 2 of the Convention of the European Council on Cybercrime (23.11.2001, ETS No. 185) defines:

"… the term "child pornography" shall include pornographic material that visually depicts:

a. a minor engaged in sexually explicit conduct;
b. a person appearing to be a minor engaged in sexually explicit conduct;
c. realistic images representing a minor engaged in sexually explicit conduct."

According to Art. 9 subsec. 3 of the Cybercrime Convention „child" is any person under 18 years of age. The Convention does not provide a definition of the term „pornographic".

In contrast to the European instruments German law does not provide a definition of the term child pornography, but differentiates between written material and pornographic performances.

---

[164] **Section 184d PC: Distribution of pornographic performances by broadcasting, media services or telecommunications services**
Whosoever disseminates pornographic performances via broadcast, media services, or telecommunications services shall be liable pursuant to sections 184 to 184c. In cases under section 184 (1) the 1st sentence above shall not apply to dissemination via media services or telecommunications services if it is ensured by technical or other measures that the pornographic performance is not accessible to persons under eighteen years of age.

[165] BGHSt 27, 60; BVerwG AfP 2002, 257; OLG Koblenz NJW 1979, 1467.

[166] BGHSt 23, 40.

[167] *König*, Kinderpornografie im Internet, p. 84 ss.

The EU Directive (2011) as the latest instrument on child pornography introduces certain regulations on specific problems concerning the ambit of regulations on child pornography that are under discussion in Germany. Examples for such problems are the topic of persons that only appear to be a child or „realistic images of a child", that in fact do not show real children. Another main difference between the European Directive and German Criminal Law lies in the definition of the term „child". Whereas under German Criminal Law a child is a person under the age of 14, both of the European legal instruments define persons under the age of 18 as children.

v. Is secondary victimization avoided for victims of child pornography in your penal law? In States where prostitution or the appearance in pornography is punishable under national criminal law, it should be possible not to prosecute or impose penalties under those laws where the child concerned has committed those acts as a result of being victim of sexual exploitation or where the child was compelled to participate in child pornography. Is this what your criminal law contemplates?

The German Law on Criminal Procedure provides some safeguards for the rights of victims of child pornography that aim at the avoidance of secondary victimization:

- Section 247 Act of Criminal Procedure: Removal of the Defendant from the Courtroom[168]
- Section 247a Act of Criminal Procedure: Witness Examination in Another Place[169]
- Section 171b Courts Constitution Act: Closed Sessions[170]

[168] Section 247 Code of Criminal Procedure: Removal of the Defendant from the Courtroom
The court may order that the defendant leave the courtroom during an examination if it is to be feared that a co-defendant or a witness will not tell the truth when examined in the presence of the defendant. The same shall apply if, on examination of a person under 18 years of age as a witness in the defendant's presence, considerable detriment to the well-being of such witness is to be feared or if an examination of another person as a witness in the defendant's presence poses an imminent risk of serious detriment to that person's health. The defendant's removal may be ordered for the duration of discussions concerning the defendant's condition and his treatment prospects, if substantial detriment to his health is to be feared. When the defendant is present again the presiding judge shall inform him of the essential contents of the proceedings, including the testimony, during his absence.

[169] **Section 247a Code of Criminal Procedure: Witness Examination in Another Place**
If there is an imminent risk of serious detriment to the well-being of the witness were he to be examined in the presence of those attending the main hearing, the court may order that the witness remain in another place during the examination; such an order shall also be admissible under the conditions set out in Section 251 subsection (2), insofar as this is necessary to establish the truth. The decision shall be incontestable. A simultaneous audio-visual transmission of the testimony shall be provided in the courtroom. The testimony shall be recorded if there is a concern that the witness will not be available for examination at a future main hearing and the recording is necessary for establishing the truth. Section 58a subsection (2) shall apply mutatis mutandis.

[170] **Sec. 171b Courts Constitution Act**
(1) The public may be excluded if circumstances from the private sphere of a participant in the proceedings, a witness or a person aggrieved by an unlawful act (section 11 subsection (1), number 5, of the Criminal Code) are mentioned, the public discussion of which would violate interests that are worthy of protection, unless there is an overriding interest in public discussion of these circumstances. This shall not apply if the persons whose private sphere is affected object to exclusion of the public in the main hearing.
(2) The public shall be excluded if the preconditions of subsection (1), first sentence, exist and the person whose private sphere is affected applies for such exclusion.
(3) The decisions pursuant to subsections (1) and (2) shall not be contestable.

- Section 395 subsec. 1a Code of Criminal Procedure: Right to Join as a Private Accessory Prosecutor[171]
- Sec. 397a subsec. 1 Code of Criminal Procedure: Appointment of an Attorney as Counsel[172]

vi. Does your criminal law criminalize "virtual child" pornography? "Virtual child" pornography does not use real children or images of real identifiable children. When the image is not that of a real child, but a combination of millions of computer pixels crafted by an artist, can the government in your country ban this allegedly victimless creation? Please cite the applicable law and/or court decisions.

Yes, virtual child pornography falls within the scope of sec. 184b PC. The term written material encompasses virtual child pornography[173]. Fictional „performances" can be written documents under sec. 184b if they display sexual activities that seem realistic and give the impression of children involved in sexual activities or of child abuse[174]. The legislator aims at the combat of the „business" of child pornography as a whole by criminalizing the consuming of such material as far as possible. Since the consuming of fictional material on child abuse supports the business of commercial child pornography at least indirectly, punishment is stretched as far as possible[175]. Still, the prerequisite that the material must give the impression of „real" activities of „real children" has the effect that most of the virtual material (as for example concerning „second life") will not fall within the purview of the offence description. Yet, in some cases punishability as dissemination under sec. 184b subsec. 1 PC might occur.

As for the blocking or erasure of child pornography by state institutions see (C) (c) 1. a. ii. 2.

vii. Mens rea: To be liable, the person should both intend to enter a site where child pornography is available and know that such images can be found there. Penalties should not be applied to persons

---

Section 172 Courts Constitution Act
The court may exclude the public from a hearing or from a part thereof if
1. endangerment of state security, the public order or public morals is to be feared,
1a. endangerment of the life, limb or liberty of a witness or another person is to be feared,
2. an important business, trade, invention or tax secret is mentioned, the public discussion of which would violate overriding interests worthy of protection,
3. a private secret is discussed, the unauthorised disclosure of which by a witness or expert carries a penalty,
4. a person under the age of 18 is examined.

[171] **Section 395 Code of Criminal Procedure: Right to Join as a Private Accessory Prosecutor**
(1) Whoever is aggrieved by an unlawful act pursuant to
1. sections 174 to 182 of the Criminal Code, …
may join a public prosecution or an application in proceedings for preventive detention as private accessory prosecutor.

[172] **Section 397a Code of Criminal Procedure: Appointment of an Attorney as Counsel**
(1) Upon application of the private accessory prosecutor an attorney shall be appointed as his counsel if he
1. has been aggrieved by a felony pursuant to sections 176a, 177, 179, 232 and 233 of the Criminal Code; …

[173] *Fischer,* § 184b marginal no. 5; S/S-*Perron/Eisele,* § 184b marginal no. 3b; *Wolters,* in: SK-StGB, § 184b marginal no. 2.

[174] S/S-*Perron/Eisele*, § 184b marginal no. 11.

[175] BT-Drucks. 12/3001, p. 5.

inadvertently accessing sites containing child pornography. Are these the requirements of your criminal law?

Sec. 184b PC requires the perpetrator's intention to access child pornography. According to sec. 184b subsec. 4 this requires the perpetrator's intent as to the age of the child as well as to the pornographic character of the displayed material. Moreover, the perpetrator's intention has to comprise the possession of pornographic material. As far as this intention presupposes the user's knowledge of the cache-functions of the used computer, his criminal intention might depend upon his technical knowledge[176].

A negligent possession of child pornography is not punishable under German criminal law.

However, the unlawful omission of an erasure of negligently obtained child pornography material can amount to a criminal offence as soon as the user has realized the formerly unknown storage of such data on his computer[177].

b. Any other object where criminalization depends on the use of Information & Communication Technologies (ICT)

Does your criminal law penalize the following conducts? Please cite the relevant law.

1. creation and use of true anonymity sending and/or receiving material on the ICT?

Anonymous communication by use of ICT is not punishable under German Criminal Law.

2. cyber-bullying?

A provision dedicated explicitly to cyber-bullying does not exist. Due to the increasing importance of this phenomenon, the public and the press sometimes demand such provisions. However, most of the cyber-bullying-cases will include the commission of existing criminal offences, as for example „using threats or force to cause a person to do, suffer or omit an act" (sec. 240 PC), threatening the commission of a felony (sec. 241 PC), insult (sec. 185 PC) or (intentional) defamation (sec. 186, 187 PC).

3. cyber-stalking?

Cyber-stalking can be punishable under sec. 238 PC[178]. The provision was introduced in the year 2007[179] with the aim to improve the protection of victims, as for the specific phenome-

[176] MüKo-*Hörnle*, § 184b marginal no. 43.
[177] *Harms*, Neue Zeitschrift für Strafrecht 2003, 646, 647; MüKo-*Hörnle*, § 184b marginal no. 37.
[178] **Section 238 PC: Stalking**
(1) Whosoever unlawfully stalks a person by
1. seeking his proximity,

non of stalking was not criminalized explicitly in the Criminal Code. The conduct of stalking could only be prosecuted if offences of the core criminal law – like trespassing or insult – were committed as well.

Concerning cyber-stalking in particular, sec. 238 subsec. 1 no. 2 PC is of special relevance: It criminalizes stalking by use of telecommunication means which includes the sending of e-mail-messages and the establishment of contacts via social networks or in chat-rooms[180].

It has to be pointed out that the behaviour is only criminalized if it leads to a significant damage to the victim's daily life. On the other hand it is punishable under sec. 238 subsec. 1 no. 2 PC already if the perpetrator confines himself to the mere attempt to establish a contact to the victim. It is not necessary that a real contact between perpetrator and victim was established[181]. However, since a considerable impairment of the victim's daily life is one condition of the offence, it is at least necessary that the victim somehow knows about the perpetrator's endeavour.[182]

4. cyber-grooming?

see (C) (c) 1. a. iii.

2. Act - creation/accession/possession/transfer/public distribution by ICT (give examples) Cite specific laws that criminalize the creation (even if never used), the accession, the possession (even if only in private), the transfer, and the public distribution through the internet and other electronic means of material beside those already mentioned above, specifically because of internet/electronic technology use.

- Sec. 86 PC Dissemination of propaganda material of unconstitutional organisations

---

2. trying to establish contact with him by means of telecommunications or other means of communication or through third persons,
3. abusing his personal data for the purpose of ordering goods or services for him or causing third persons to make contact with him,
4. threatening him or a person close to him with loss of life or limb, damage to health or deprivation of freedom, or
5. committing similar acts

and thereby seriously infringes his lifestyle shall be liable to imprisonment not exceeding three years or a fine.
(2) The penalty shall be three months to five years if the offender places the victim, a relative of or another person close to the victim in danger of death or serious injury.
(3) If the offender causes the death of the victim, a relative of or another person close to the victim the penalty shall be imprisonment from one to ten years.
(4) Cases under subsection (1) above may only be prosecuted upon request unless the prosecuting authority considers propio motu that prosecution is required because of special public interest.

[179] 2007 Federal Law Gazette I, p. 354.
[180] *Peters*, Der Tatbestand des § 238 StGB (Nachstellung) in der staatsanwaltlichen Praxis, Neue Zeitschrift für Strafrecht 2009, 238, 240.
[181] NK-*Bernd-Rüdeger/Sonnen*, § 238 marginal no. 34.
[182] S/S-*Eisele*, § 238 marginal no. 11.

- Sec. 86a PC Using symbols of unconstitutional organisations
- Sec. 91 PC Encouraging the commission of a serious violent offence endangering the state
- Sec. 111 PC Public incitement to crime
- Sec. 130 PC Incitement to hatred
- Sec. 130a PC Attempting to cause the commission of offences by means of publication
- Sec. 131 PC Dissemination of depictions of violence
- Sec. 284 PC Organising unlawful gaming
- Sec. 287 PC Organising an unlawful lottery etc.
- Offences implying the disclosure of private secrets/communication: Sec. 203 PC Violation of private secrets; sec. 206 PC Violation oft he postal and telcommunications secret, sec. 353b PC Breach of official secrets and special duties of confidentiality
- Infringement of Copyrights: Sec. 106 Copyright Act Unlawful exploitation of copyrighted works; sec. 108 Copyright Act Infringement of related rights; sec. 108b Copyright Act Infringement of technological measures and rights-management information

(d) ICT Related Violations of Property, Including Intellectual Property

Does your criminal law specifically proscribe and penalize the following conducts perpetrated through the use of the ICT? Please, cite the relevant law.

1. Fraud

Yes, see

Section 263a PC: Computer fraud
(1) Whosoever with the intent of obtaining for himself or a third person an unlawful material benefit damages the property of another by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorised use of data or other unauthorised influence on the course of the processing shall be liable to imprisonment not exceeding five years or a fine.
(2) Section 263(2) to (7) shall apply mutatis mutandis.
(3) Whosoever prepares an offence under subsection (1) above by writing computer programs the purpose of which is to commit such an act, or procures them for himself or another, offers them for sale, or holds or supplies them to another shall be liable to imprisonment not exceeding three years or a fine. …

See also
Section 265a PC: Obtaining services by deception
(1) Whosoever obtains the service of a machine or a telecommunications network serving public purposes or uses a means of transportation or obtains entrance to an event or institution by deception with the intent of not paying for them shall be liable to imprisonment not exceeding one year or a fine unless the act is punishable under other provisions with a more severe penalty.
(2) The attempt shall be punishable. …

2. Infringement of Intellectual Property IP rights

Article 106 Copyright Act: Unlawful exploitation of copyrighted works
(1) Anyone who without the consent of the rightholder reproduces, distributes or communicates to the public a work or an adaptation or transformation of a work in manners other than those permitted by law shall be liable to imprisonment of not more than 3 years or a fine.
(2) Any attempt shall be punishable.

Article 107 Copyright Act: Unlawful affixing of designation of author
(1) Any person who
1. without the consent of the author affixes to the original of an artistic work the designation of author (Article 10 (1)) or distributes an original bearing such designation,
2. affixes to a copy, an adaptation or transformation of an artistic work the designation of author (Article 10 (1)) in a manner which gives the copy, adaptation or transformation the appearance of an original, or distributes a copy, such an adaptation or transformation bearing such designation,
shall be liable to imprisonment of not more than three years or a fine, unless other provisions impose a more serious sentence.
(2) Any attempt shall be punishable.

Article 108 Copyright Act: Infringement of related rights
(1) Any person who without the consent of the rightholder
1. reproduces, distributes or communicates to the public a scientific edition (Article 70) or an adaptation or transformation of such an edition,
2. exploits a posthumous work or an adaptation or transformation of such a work contrary to Article 71,
3. reproduces, distributes or communicates to the public a photograph (Article 72) or an adaptation or transformation of a photograph,
4. exploits a performance by a performer contrary to Article 77 (1) or (2), first sentence, Article 78 (1),
5. exploits an audio recording contrary to Article 85,
6. exploits a broadcast contrary to Article 87,
7. exploits a video recording or a video and audio recording contrary to Articles 94 or 95 read in conjunction with Article 94,
8. exploits a database contrary to Article 87b (1),
in manners other than those permitted by law shall be liable to imprisonment of not more than three years or a fine.
(2) Any attempt shall be punishable.

Article 108a Copyright Act: Unlawful exploitation on a commercial scale
(1) Where the offender in the cases referred to in Articles 106 to 108 acts on a commercial basis, the penalty shall be imprisonment of not more than five years or a fine.
(2) Any attempt shall be punishable.

Article 108b Copyright Act: Infringement of technological measures and rights-management information
(1) Any person who, 1. with the intention of enabling for himself or a third party access to a work which is protected under this Act or to other subject-matter protected under this Act or its exploitation, circumvents an effective technological measure without the consent of the rightholder, or 2. knowingly without authorisation a) removes or alters rights-management information provided by rightholders, if any of the information concerned is affixed to a copy of a work or of other protected subject-matter, or is released in the context of the communication to the public of such a work or protected subject-matter, or b) distributes, imports for distribution, broadcasts, communicates to the public or makes available to the public a work or other protected subject-matter where rights-

management information was removed or altered without authorisation by doing so, has at least carelessly induced, enabled, facilitated or concealed an infringement of copyright or related rights, if the offence was not committed exclusively for the personal private use of the offender or of persons personally associated with the offender or does not relate to such use, shall be liable to imprisonment of not more than one year or a fine.
(2) Punishment shall also be imposed on any person who in violation of Article 95a (3) produces, imports, distributes, sells or rents a device, a product or component for commercial purposes.
(3) If in cases under paragraph (1) the offender acts on a commercial scale, the penalty shall be imprisonment of not more than three years or a fine.

Similar Provisions are included in the German Acts on Trademarks, on Patents and on Design Patents.

3. Industrial espionage

Section 17 Act Against Unfair Competition: Disclosure of trade and industrial secrets
(1) Whoever as the employee of a business communicates, without authorisation, a trade or industrial secret with which he was entrusted, or to which he had access, during the course of the employment relationship to another person for the purposes of competition, for personal gain, for the benefit of a third party, or with the intent of causing damage to the owner of the business shall be liable to imprisonment not exceeding three years or to a fine.
(2) Whoever for the purposes of competition, for personal gain, for the benefit of a third party, or with the intent of causing damage to the owner of the business, acquires or secures, without authorisation,
1. a trade or industrial secret
a) by using technical means;
b) by creating an embodied communication of the secret; or
c) by removing an item in which the secret is embodied; or
2. without authorisation, uses or communicates to anyone a trade secret which he acquired through one of the communications referred to in subsection (1), or through an act of his own or of a third party pursuant to number 1, or which he has otherwise acquired or secured without authorisation shall incur the same liability.
(3) An attempt shall incur criminal liability.
(4) In particularly serious cases the sentence shall consist in imprisonment not exceeding five years or a fine. A particularly serious case shall usually exist in circumstances where the perpetrator
1. acts on a commercial basis;
2. knows at the time of the communication that the secret is to be used abroad; or
3. himself effects a use pursuant to subsection (2), number 2, abroad.
(5) The offence shall be prosecuted upon application only, unless the criminal prosecution authority considers that it is necessary to take ex officio action on account of the particular public interest in the criminal prosecution.

(e) Criminalization of Acts Committed in the Virtual World

Does your criminal law penalize the commission of crimes committed in the virtual world like, for example, virtual child pornography, virtual violence, virtual graffiti, cyber-defamation, sexual harassment, harassment at work, without any involvement of real persons, only virtual representation? Please site the relevant law and provide details.

As for virtual child pornography see (C)(c)1.a.vi.

The dissemination of material containing virtual/fictional violence is criminalized under sec. 184a PC, as far as pornographic violence is concerned[183] - see (C)(c)1.a.vi.

In some cases displaying of fictional/virtual violence might result in an offence under sec. 131 PC[184]. The ambit of the offence was extended to „humanoid beings" in order to include virtual descriptions of violence[185]. While displaying violence itself does not suffice to meet the offence requirements, the display of violence being performed in a manner expressing glorification or playing acts of violence down or violating human dignity qualifies the act as an offence.

Virtual graffity is not criminalized explicitly under German criminal law. As far as virtual graffity leads to an alteration of data, the offence of sec. 303a PC (data tampering) is relevant.

Since virtual personalities – as represented by the avatars of internet users – are not protected under German criminal law, personal insult under sec. 185 PC can only be committed if it can be traced back to the natural person represented by the avatar.

The same is true for sexual harassment. A sexual assault (sec. 177 subsec. 1 PC) can only be committed to the detriment of a natural person.

(f) Non-Compliance Offenses

Does your criminal law penalize non cooperation with law enforcement agencies in the field of cybercrime? Duties to cooperate can be duties to retain and store information, to produce/deliver information as required by a production order, to give access to cyber systems to install filters or devices, etc. Is the breach of the duty to cooperate also enforced through administrative sanctions? Cite the relevant law and provide details.

[183] S/S-*Perron/Eisele,* § 184a marginal no. 3.

[184] **Section 131 PC: Dissemination of depictions of violence**
(1) Whosoever
1. disseminates written materials (section 11(3)), which describe cruel or otherwise inhuman acts of violence against humans or humanoid beings in a manner expressing glorification or which downplays such acts of violence or which represents the cruel or inhuman aspects of the event in a manner which violates human dignity;
2. publicly displays, posts, presents, or otherwise makes them accessible;
3. offers, supplies or makes them accessible to a person under eighteen years; or
4. produces, obtains, supplies, stocks, offers, announces, commends, undertakes to import or export them, in order to use them or copies obtained from them within the meaning of numbers 1 to 3 above or facilitate such use by another,
shall be liable to imprisonment not exceeding one year or a fine.
(2) Whosoever disseminates a presentation with a content indicated in subsection (1) above by radio, media services, or telecommunication services shall incur the same penalty.
(3) Subsections (1) and (2) above shall not apply in cases of reporting about current or historical events.
(4) Subsection (1) No 3 above shall not apply if the person authorised to care for another person acts; this shall not apply if that person grossly neglects his duty of education by offering, giving, or making them accessible.

[185] BT-Drucks. 15/1311, p. 22.

Service providers are allowed to collect and use customer and traffic data to the extent required for performance of the contract between the service providers, sec. 95[186], 96[187] Tele-

[186] **Section 95 Telecommunications Act: Contractual Relations**
(1) The service provider may collect and use customer data to the extent required to achieve the purpose referred to in section 3 para 3. Under a contractual relationship with another service provider, the service provider may collect and use the customer data of his subscribers and of the subscribers of the other service provider to the extent required for performance of the contract between the service providers. Transmission of the customer data to third parties, unless permitted by this Part or by another law, shall be carried out only with the subscriber's consent.
(2) The service provider may use the customer data of the subscribers referred to in subsection (1) sentence 2 for subscriber advisory purposes, for promoting his own offerings and for market research only to the extent required for such purposes and provided the subscriber has given his consent. A service provider who, under an existing customer relationship, has lawfully received notice of a subscriber's telephone number or postal address, including his electronic address, may use these for the transmission of text or picture messages to a telephone or postal address for the purposes referred to in sentence 1, unless the subscriber has objected to such use. Use of the telephone number or address according to sentence 2 shall be permitted only if the subscriber, when the telephone number or address is collected or first stored and on each occasion a message is sent to such telephone number or address for one of the purposes referred to in sentence 1, is given information in clearly visible and well readable form that he may object at any time, in writing or electronically, to the dispatch of further messages.
(3) When the contractual relationship ends, the customer data are to be erased by the service provider upon expiry of the calendar year following the year in which the contract terminated. Section 35(3) of the Federal Data Protection Act applies accordingly.
(4) In connection with the establishment of, or modification to, a contractual relationship or with the provision of telecommunications services, the service provider may require presentation of an official identity card where this is necessary to verify the subscriber's particulars. The service provider may make a copy of the identity card. The copy is to be destroyed by the service provider without undue delay once the particulars needed for the conclusion of the contract have been established. The service provider may not use data other than the data permitted under subsection (1).
(5) The provision of telecommunications services may not be made dependent upon the subscriber's consent to use of his data for other purposes where the subscriber is not able, or is not able in reasonable manner, to access such telecommunications services in another way.

[187] **Section 96 Telecommunications Act: Traffic Data**
(1) The service provider may collect and use the following traffic data to the extent required for the purposes set out in this Chapter
1. the number or other identification of the lines in question or of the terminal, personal authorisation codes, additionally the card number when customer cards are used, additionally the location data when mobile handsets are used;
2. the beginning and end of the connection, indicated by date and time and, where relevant to the charges, the volume of data transmitted;
3. the telecommunications service used by the user; 4. the termination points of fixed connections, the beginning and end of their use, indicated by date and time and, where relevant to the charges, the volume of data transmitted;
5. any other traffic data required for setup and maintenance of the telecommunications connection and for billing purposes.
(2) Stored traffic data may be used after the termination of a connection only where required to set up a further connection or for the purposes referred to in sections 97, 99, 100 and 101. Otherwise, traffic data are to be erased by the service provider without undue delay following termination of the connection.
(3) The service provider may use subscriber-related traffic data used by the provider of a publicly available telecommunications service for the purpose of marketing telecommunications services, shaping telecommunications services to suit the needs of the market or for the provision of value added services for the duration necessary only where the data subject has given his consent to such use. The data of the called party are to be made anonymous without undue delay. Traffic data relating to the destination number may be used by the service provider for the purpose referred to in sentence 1 only with the consent of the called party. In such case, the called party data are to be made anonymous without undue delay.

communications Act. Apart from the general *right* to store the data, sec. 111 Telecommunications Act[188] establishes an *obligation* to store the data to some extent. In this regard, sec. 112 Telecommunications Act[189] stipulates a duty for service providers to ensure that the relevant

---

(4) When obtaining consent, the service provider is to inform the subscriber of the data types which are to be processed for the purposes referred to in subsection (3) sentence 1 and of the storage duration. Additionally, the subscriber's attention is to be drawn to the possibility of withdrawing his consent at any time.

[188] **Section 111 Telecommunications Act: Data for Information Requests from Security Authorities**

(1) Any person commercially providing or assisting in providing telecommunications services and in so doing allocating telephone numbers or providing telecommunications connections for telephone numbers allocated by other parties is, for the information procedures according to sections 112 and 113, to collect, prior to activation, and store without undue delay the telephone numbers, the name and address of the allocation holder, the effective date of the contract, the date of birth in the case of natural persons, and in the case of fixed lines, additionally the address for the line, even if such data are not required for operational purposes; where known, the date of termination of the contract is likewise to be stored. Sentence 1 also applies where the data are not included in directories of subscribers (section 104). A person with obligations according to sentence 1 receiving notice of any changes is to correct the data without undue delay; in this connection the person with obligations is subsequently to collect and store data according to sentence 1 not yet recorded if collecting the data is possible at no special effort. When the contractual relationship ends, the data are to be erased upon expiry of the calendar year following the year in which the contract terminated. Compensation for data collection and storage is not paid. The manner in which data for the information procedure according to section 113 are stored is optional.

(2) Where the service provider according to subsection (1) sentence 1 operates in conjunction with a sales partner, such partner shall collect data according to subsection (1) sentence 1 and transmit to the service provider, without undue delay, these and data collected under section 95; subsection (1) sentence 2 applies accordingly. Sentence 1 also applies to data relating to changes, inasmuch as the sales partner receives notice of them in the course of normal business transactions.

(3) Data within the meaning of subsection (1) sentence 1 need not be collected subsequently for contractual relationships existing on the date of entry into force of this provision, save in the cases referred to in subsection (1) sentence 3.

[189] **Section 112 Telecommunications Act: Automated Information Procedure**

(1) Any person providing publicly available telecommunications services shall store, without undue delay, data collected under section 111(1) sentences 1 and 3 and subsection (2) in customer data files in which the telephone numbers and quotas of telephone numbers allocated to other telecommunications service providers for further marketing or other use and, with regard to ported numbers, the current carrier portability codes, are also to be included. Section 111(1) sentences 3 and 4 apply accordingly with regard to the correction of customer data files. In the case of ported numbers the telephone number and associated carrier portability code are not to be erased before expiry of the year following the date on which the telephone number was returned to the network operator to whom it had originally been allocated. The person with obligations shall ensure that
1. the Regulatory Authority can, at all times, retrieve from customer data files data for information requests from the authorities referred to in subsection (2) by means of automated procedures in the Federal Republic of Germany;
2. data can be retrieved using incomplete search data or searches made by means of a similarity function.
The requesting office is to consider, without undue delay, the extent to which it needs the data provided and erase, without undue delay, any data not needed. The person with obligations is to ensure by technical and organisational measures that no retrievals can come to his notice.

(2) Information from the customer data files according to subsection (1) shall be provided to
1. the courts and criminal prosecution authorities;
2. federal and state police enforcement authorities for purposes of averting danger;
3. the Customs Criminological Office and customs investigation offices for criminal proceedings and the Customs Criminological Office for the preparation and execution of measures under section 39 of the Foreign Trade and Payments Act;
4. federal and state authorities for the protection of the Constitution, the Federal Armed Forces Counter-Intelligence Office and the Federal Intelligence Service;
5. the emergency service centres according to section 108 and the service centre for the maritime mobile emergency number "124124";
6. the Federal Financial Supervisory Authority; and

data can be accessed by the Regulatory Authorities. Under sec. 113 Telecommunications Act[190] the service providers are obliged to provide competent public bodies with the demand-

---

7. the authorities responsible under state legislation for the prosecution of administrative offences as provided for by section 4(3) of the Undeclared Work Act, via central inquiry offices, as stipulated in subsection (4), at all times, as far as such information is needed to discharge their legal functions and the requests are submitted to the Regulatory Authority by means of automated procedures. (3) The Federal Ministry of Economics and Labour shall be empowered to issue, in agreement with the Federal Chancellery, the Federal Ministry of the Interior, the Federal Ministry of Justice, the Federal Ministry of Finance and the Federal Ministry of Defence, an ordinance having the force of law and requiring the consent of the German Bundesrat, in which the following matters are regulated–
1. the essential requirements in respect of the technical procedures for
a) the transmission of requests to the Regulatory Authority;
b) the retrieval of data by the Regulatory Authority from persons with obligations, including the data types to be used for the queries; and
c) transmission by the Regulatory Authority to the requesting authorities of the data retrieved;
2. the security requirements to be observed; and
3. in respect of retrievals using incomplete search data and searches made by means of similarity functions for which specifications on the character sequences to be included in the search are provided by the Ministries contributing to the ordinance,
a) the minimum requirements in respect of the extent of the data to be entered in order to identify, as precisely as possible, the person to whom the search relates;
b) the permitted number of hits to be transmitted to the requesting authority; and
c) the requirements in respect of the erasure of data not needed.
In other respects, the ordinance may also restrict the query facility for the authorities referred to Authority shall determine the technical details of the automated retrieval procedure in a technical directive to be drawn up with the participation of the associations concerned and the authorized bodies and to be brought into line with the state of the art, where required, and published by the Regulatory Authority in its Official Gazette. The person with obligations according to subsection (1) and the authorised bodies are to meet the requirements of the technical directive not later than one year following its publication. In the event of an amendment to the directive, defective-free technical facilities configured to the directive shall meet the modified requirements not later than three years following its taking effect.
(4) At the request of the authorities referred to in subsection (2), the Regulatory Authority is to retrieve and transmit to the requesting authority the relevant data sets from the customer data files according to subsection (1). It shall examine the admissibility of the transmission only where there is special reason to do so. Responsibility for such admissibility lies with the authorities referred to in subsection (2). For purposes of data protection control by the competent body, the Regulatory Authority shall record, for each retrieval, the time, the data used in the process of retrieval, the data retrieved, the person retrieving the data, the requesting authority and the reference number of the requesting authority. Use for any other purposes of data recorded is not permitted. Data recorded are to be erased after a period of one year.
(5) The person with obligations according to subsection (1) is to make all such technical arrangements in his area of responsibility as are required for the provision of information under this provision, at his expense. This also includes procurement of the equipment required to secure confidentiality and protection against unauthorised access, installation of a suitable telecommunications connection, participation in the closed user system and the continued provision of all such arrangements as are required under the ordinance and the technical directive according to subsection (3). Compensation for information provided by means of automated procedures is not paid to persons with obligations.

[190] **Section 113 Telecommuncations Act: Manual Information Procedure**
(1) Any person commercially providing or assisting in providing telecommunications services shall, in a given instance, provide the competent bodies, at their request, without undue delay, with information on data collected under sections 95 and 111 to the extent required for the prosecution of criminal or administrative offences, for averting danger to public safety or order and for the discharge of the legal functions of the federal and state authorities for the protection of the Constitution, the Federal Intelligence Service and the Federal Armed Forces Counter-Intelligence Office. The person with obligations according to sentence 1 shall provide information on data by means of which access to terminal equipment or to storage devices or units installed in such equipment or in the network is protected, notably personal identification numbers (PINs) or personal unlocking keys (PUKs), by virtue of an information request under section 161(1) sentence 1 or section 163(1) of

ed information. Apart from this, sec. 110 Telecommunications Act[191] establishes further obligations of telecommunication providers. A violation of the mentioned duties is considered an administrative offence under sec. 149 Telecommunications Act[192].

---

the Code of Criminal Procedure, data collection provisions in federal or state police legislation for averting danger to public safety or order, section 8(1) of the Federal Constitution Protection Act, the corresponding provisions of the state constitution protection legislation, section 2(1) of the Federal Intelligence Service Act or section 4(1) of the Federal Armed Forces Counter-Intelligence Act; such data shall not be transmitted to any other public or private bodies. Access to data which are subject to telecommunications privacyshall be permitted only under the conditions of the relevant legislation. The person with obligations shall maintain silence vis-à-vis his customers and third parties about the provision of information.
(2) The person with obligations according to subsection (1) is to make such arrangements as are required in his area of responsibility for the provision of information, at his expense. In respect of information provided, the person with obligations is granted compensation by the requesting authority, the level of which, in derogation of section 17a(1) para 2 of the Reimbursement of Witnesses and Experts Act, is determined by the ordinance referred to in section 110(9). Sentence 2 also applies in those cases in which, under the manual information procedure, merely data are requested which the person with obligations also keeps available for retrieval under the automated information procedure according to section 112. Sentence 2 does not apply in those cases in which the information was not provided completely or was not provided correctly under the automated information procedure according to section 112.

[191] **Section 110 Telecommunications Act: Technical Implementation of Intercepts**
(1) Any person operating a telecommunications system by means of which publicly available telecommunications services are provided, shall,
1. from the time of beginning operation, at his own expense, provide technical facilities with which to implement telecommunications interception measures provided for by law and make organisational arrangements for the implementation, without undue delay, of such measures;
2. without undue delay after beginning operation, vis-à-vis the Regulatory Authority,
a) declare that he has made the arrangements according to para 1; and
b) nominate a body located in the Federal Republic of Germany to receive judicial orders destined for him, relating to telecommunications interception;
3. demonstrate to the Regulatory Authority, at no charge, that the technical facilities and organisational arrangements according to para 1 are compliant with the provisions of the ordinance according to subsection (2) and the technical directive according to subsection (3); to this end, he shall, without undue delay but not later than one month after beginning operation,
a) send to the Regulatory Authority the documents needed to prepare the checks the Regulatory Authority carries out to verify compliance; and
b) agree with the Regulatory Authority a date for demonstrating and verifying compliance;
he shall assist the Regulatory Authority in the checks required for verifying compliance;
4. allow the Regulatory Authority, at its special request in a given, justified instance, to re-check, at no charge, his technical and organisational arrangements; and
5. tolerate the installation and operation on his premises of equipment for the implementation of measures under sections 5 and 8 of the Article 10 Act and grant staff of the office responsible for such measures and members and staff of the G10 Commission (section 1(2) of the Article 10 Act) access to such equipment for the discharge of their legal functions. Any person offering publicly available telecommunications services without themselves operating a telecommunications system to do so shall, when choosing the operator of the telecommunications system to be used for doing so, make certain that the latter can carry out judicial orders relating to telecommunications interception without undue delay as provided for by the ordinance according to subsection (2) and by the technical directive according to subsection (3), and notify the Regulatory Authority without undue delay after beginning to provide service of which telecommunications services he is offering, by whom judicial intercept orders concerning his subscribers are to be carried out and to which body located in the Federal Republic of Germany judicial orders relating to telecommunications interception are to be addressed. Any changes in the data on which the notifications according to sentence (1) para (2) b) and sentence 2 are based are to be notified to the Regulatory Authority without undue delay. In cases in which provisions according to subsection (3) are not yet available, the person with obligations shall configure the technical facilities according to sentence 1 para 1 in agreement with the Regulatory Authority. Sentences 1 to 4 do not apply where the ordinance according to subsection (2) provides for exemptions with regard to the telecommunica-

tions system. Section 100b(3) sentence 1 of the Code of Criminal Procedure, section 2(1) sentence 3 of the Article 10 Act and the relevant state regulations on preventive telecommunications interception by the police remain unaffected.
(2) The Federal Government shall be empowered
1. to make arrangements concerning
a) the technical essential requirements and the organisational key elements for the implementation of intercepts, including the implementation of intercepts by a person acting on behalf of the person with obligations;
b) the extent of the arrangements in the technical directive according to subsection (3);
c) demonstration of compliance as provided for by subsection (1) sentence 1 paras 3 and 4; and
d) details of the obligation of tolerance as required by subsection (1) sentence 1 para 5; and
2. to determine
a) the cases in which and the conditions under which compliance with certain technical requirements can be dispensed with on a temporary basis;
b) that the Regulatory Authority may, for technical reasons, allow exemptions in respect of meeting particular technical requirements; and
c) in respect of which telecommunications systems and associated service offers technical facilities need not be offered or organisational measures need not be taken, in derogation of subsection (1) sentence 1 para 1, on account of basic technical considerations or for reasons of proportionality, by ordinance having the force of law and requiring the consent of the German Bundesrat.
(3) The Regulatory Authority shall stipulate, in a technical directive to be drawn up in consultation with the authorised bodies and with the participation of industry associations and manufacturers, the technical details required to guarantee a full record of telecommunications intercepts and for configuration of the point of handover to the authorised bodies. International technical standards are to be taken into consideration; reasons for deviations from the standards are to be stated. The technical directive is to be published by the Regulatory Authority in its Official Gazette.
(4) Any person manufacturing or distributing technical facilities for the implementation of intercepts may require the Regulatory Authority to verify, by testing the interworking of a type sample with particular telecommunications systems, whether or not the legal and technical provisions of the ordinance according to subsection (2) and of the technical directive according to subsection (3) have been met. The Regulatory Authority may, after due assessment of the circumstances, allow deviations from the technical requirements on a temporary basis, provided that implementation of the intercepts is secured in principle and only insignificant adjustments to the technical facilities of the authorised bodies are required. The Regulatory Authority is to notify the manufacturer or distributor in writing of the test results. The test results are noted by the Regulatory Authority in connection with the demonstration of compliance of the technical facilities with the applicable technical provisions which the person with obligations is required to provide under subsection (1) sentence 1 para 3 or 4. Consent to the framework concepts presented by manufacturers given by the Federal Ministry of Economics and Labour prior to the entry into force of this provision is deemed notification within the meaning of sentence 3.
(5) Any person obliged under subsection (1) in conjunction with the ordinance according to subsection (2) to make arrangements is to meet the requirements of the ordinance and the technical directive according to subsection (3) not later than one year following their publication, unless a longer period has been determined there for particular obligations. Defective-freetechnical facilities configured to this directive for telecommunications services already offered by the person with obligations shall, in the event of an amendment to the directive, meet the modified requirements not later than three years following its taking effect. Where shortcomings in the technical or organisational arrangements of the person with obligations are found in the process of compliance according to subsection (1) sentence 1 para 3 being demonstrated or a re-check according to subsection (1) sentence 1 para 4 being made, the person with obligations is to eliminate such shortcomings within a reasonable period of time as provided for by the Regulatory Authority; where shortcomings are found during operations, notably when intercepts are carried out, the person with obligations is to eliminate such shortcomings without undue delay. If type samples have been tested under subsection (4) for the technical facilities and deadlines set for the elimination of shortcomings, the Regulatory Authority shall take these deadlines into account in its specifications on the elimination of shortcomings according to sentence 3.
(6) Every operator of a telecommunications system renting to third parties network termination points in his telecommunications system under his publicly available service offer shall undertake to make available to the bodies authorised by law to carry out telecommunications intercepts, without undue delay and as a matter of

Law enforcement authorities are granted the right to collect traffic data under sec. 96 Telecommunications Act[193] by sec. 100g Code of Criminal Procedure[194]. Service providers are

priority, at their request, network termination points for transmission of the information obtained under an intercept. The technical configuration of such termination points may be laid down in the ordinance according to subsection (2). With the exception of special tariffs or surcharges for priority or early provision or fault repair, the tariffs payable by the general public apply in respect of such provision and use. Any special contractually agreed discounts remain unaffected by sentence 3.
(7) Telecommunications systems operated by legally authorised bodies and by means of which intervention in the privacy of telecommunications or in network operation is to be brought about, are to be technically configured in agreement with the Regulatory Authority. The Regulatory Authority is to comment on the technical configuration within a reasonable period of time.
(8) Operators of telecommunications systems with obligations under sections 100a and 100b of the Code of Criminal Procedure are to prepare, and make available to the Regulatory Authority at no charge, annual statistics of intercepts carried out under these provisions. The presentation of these statistics may be detailed in the ordinance according to subsection (2). Operators shall not disclose the statistics to third parties. The Regulatory Authority shall aggregate the data provided by the undertakings and publish the result in its Official Gazette annually.
(9) The Federal Government shall be empowered to make arrangements, by ordinance having the force of law and requiring the consent of the German Bundestag and the German Bundesrat, with regard to appropriate compensation to be paid to service providers for services supplied by them in
1. enabling intercepts under sections 100a and 100b of the Code of Criminal Procedure, section 2(1), section 5 or section 8 of the Article 10 Act, section 39 of the Foreign Trade and Payments Act or the relevant state regulations, and
2. providing information in accordance with section 113.
The costs of providing technical facilities as required to provide the services according to sentence 1 are not the subject of such compensation arrangements.

[192] **Section 149 Telecommunications Act: Administrative Fines Provisions**
(1) An administrative offence is deemed to have been committed by any person who, intentionally or negligently,
22. in contravention of section 110(1) sentence 1 para 1 in conjunction with an ordinance according to section 110(2) para 1 a), fails to provide a technical facility or to make organisational arrangements;
23. in contravention of section 110(1) sentence 1 para 2 b), fails to nominate a body as named there or to nominate it in timely manner;
24. in contravention of section 110(1) sentence 1 para 3, fails to demonstrate compliance or to demonstrate it in timely manner;
25. in contravention of section 110(1) sentence 1 para 4, fails to allow a re-check;
26. in contravention of section 110(1) sentence 1 para 5, fails to tolerate the installation or operation of equipment referred to there or to grant access to such equipment;
27. in contravention of section 110(5) sentence 3, fails to eliminate shortcomings or to eliminate them in timely manner;
28. in contravention of section 110(6) sentence 1, fails to make available a network termination point, to make it available as prescribed or to make it available in timely manner;
29. in contravention of section 111(1) sentence 1, also in conjunction with sentence 2, or in contravention of section 111(1) sentence 3 or 4, fails to collect data or to collect them in timely manner, fails to store data or to store them in timely manner, fails to correct data or to correct them in timely manner or fails to erase data or to erase them in timely manner;
30. in contravention of section 111(2) sentence 1, also in conjunction with sentence 2, fails to collect data or to collect them in timely manner or fails to transmit data or to transmit them in timely manner;
31. in contravention of section 112(1) sentence 4, fails to ensure that the Regulatory Authority can retrieve data from customer data files;
32. in contravention of section 112(1) sentence 6, fails to ensure that no retrievals can come to his notice;
33. in contravention of section 113(1) sentence 1 or 2, section 114(1) sentence 1 or section 127(1) sentence 1, fails to provide information, to provide it correctly, to provide it completely or to provide it in timely manner;
34. in contravention of section 113(1) sentence 2 second half-sentence, transmits data; or
35. in contravention of section 113(1) sentence 4, fails to maintain silence.

[193] See footnote 188.

obliged to cooperate with the authorities insofar and are obliged to provide information on request without undue delay. In case the service providers object to such disclosure, the law enforcement agencies have several regulatory and coercive measures at their disposal, sec. 100b subsec. 3, 95 subsec. 2 Code of Criminal Procedure[195]. Moreover, the denial of information can amount to an offence under sec. 258 PC[196] - assistance in avoiding prosecution or punishment.

---

[194] **Section 100g Code of Criminal Procedure: Information on Telecommunications Connections**
(1) If certain facts give rise to the suspicion that a person, either as perpetrator or as inciter or accessory,
1. has committed a criminal offence of substantial significance in the individual case as well, particularly one of the offences referred to in Section 100a subsection (2), or, in cases where there is criminal liability for attempt, has attempted to commit such an offence or has prepared such an offence by committing a criminal offence, or
2. has committed a criminal offence by means of telecommunication,
then, to the extent that this is necessary to establish the facts or determine the accused's whereabouts, telecommunications traffic data (section 96 subsection (1), section 113a of the Telecommunications Act) may be obtained also without the knowledge of the person concerned. In the case referred to in the first sentence, number 2, the measure shall be admissible only where other means of establishing the facts or determining the accused's whereabouts would offer no prospect of success and if the acquisition of the data is proportionate to the importance of the case. The acquisition of location data in real time shall be admissible only in the case of the first sentence, number 1.
(2) Section 100a subsection (3) and Section 100b subsections (1) to (4), first sentence, shall apply mutatis mutandis. Unlike Section 100b subsection (2), second sentence, number 2, in the case of a criminal offence of substantial significance, a sufficiently precise spatial and temporal description of the telecommunication shall suffice where other means of establishing the facts or determining the accused's whereabouts would offer no prospect of success or be much more difficult.
(3) If the telecommunications traffic data is not acquired by the telecommunications services provider, the general provisions shall apply after conclusion of the communication process.
(4) In accordance with Section 100b subsection (5) an annual report shall be produced in respect of measures pursuant to subsection (1), specifying
1. the number of proceedings during which measures were implemented pursuant to subsection (1);
2. the number of measures ordered pursuant to subsection (1) distinguishing between initial orders and subsequent extension orders;
3. in each case the underlying criminal offence, distinguishing between numbers 1 and 2 of subsection (1), first sentence;
4. the number of months elapsed during which telecommunications traffic data was intercepted, measured from the time the order was made;
5. the number of measures which produced no results because the data intercepted was wholly or partially unavailable.

[195] **Section 100b Code of Criminal Procedure: Order to Intercept Telecommunications**
(1) Measures pursuant to Section 100a may be ordered by the court only upon application by the public prosecution office. In exigent circumstances, the public prosecution office may also issue an order. An order issued by the public prosecution office shall become ineffective if it is not confirmed by the court within three working days. The order shall be limited to a maximum duration of three months. An extension by not more than three months each time shall be admissible if the conditions for the order continue to exist, taking into account the information acquired during the investigation.
… (3) On the basis of this order all persons providing, or contributing to the provision of, telecommunications services on a commercial basis shall enable the court, the public prosecution office and officials working in the police force to assist it (section 152 of the Courts Constitution Act), to implement measures pursuant to Section 100a and shall provide the required information without delay. Whether and to what extent measures are to be taken in this respect shall follow from the Telecommunications Act and from the Telecommunications Interception Ordinance issued thereunder. Section 95 subsection (2) shall apply mutatis mutandis.
Sec. 95 Code of Criminal Procedure: Obligation to Surrender
… (2) In the case of non-compliance, the regulatory and coercive measures set out in Section 70 may be used against such person. This shall not apply to persons who are entitled to refuse to testify.

[196] **Section 258 PC: Assistance in avoiding prosecution or punishment**

Apart from this, law enforcement agencies have the right to demand the disclosure of information exercising their general investigative powers under sec. 161, 163 and 95 Code of Criminal Procedure[197].

(D) Complementary optional information concerning law and practice (including statistics)

(1) Are cybercrimes included as such in the collection of data on crime in your country?

---

(1) Whosoever intentionally or knowingly obstructs in whole or in part the punishment of another in accordance with the criminal law because of an unlawful act or his being subjected to a measure (section 11(1) No 8) shall be liable to imprisonment not exceeding five years or a fine.
(2) Whosoever intentionally or knowingly obstructs in whole or in part the enforcement of a sentence or measure imposed on another shall incur the same penalty.

[197] **Section 161 Code of Criminal Procedure: Information and Investigations**
(1) For the purpose indicated in Section 160 subsections (1) to (3), the public prosecution office shall be entitled to request information from all authorities and to make investigations of any kind, either itself or through the authorities and officials in the police force provided there are no other statutory provisions specifically regulating their powers. The authorities and officials in the police force shall be obliged to comply with the request or order of the public prosecution office and shall be entitled, in such cases, to request information from all authorities.
(2) Where measures pursuant to this statute are only admissible where the commission of particular criminal offences is suspected, personal data that has been obtained as a result of a corresponding measure taken pursuant to another statute may be used as evidence in criminal proceedings without the consent of the person affected by the measure only to clear up one of the criminal offences in respect of which such a measure could have been ordered to clear up the offence pursuant to this statute. Section 100d, subsection (5), number 3 shall remain unaffected.
(3) Personal data obtained in or from private premises by technical means for the purpose of personal protection during a clandestine investigation based on police law may be used as evidence, having regard to the principle of proportionality (Article 13 paragraph (5) of the Basic Law), only after determination of the lawfulness of the measure by the Local Court (Section 162 subsection (1)) in whose district the authority making the order is located; in exigent circumstances a judicial decision is to be sought without delay.
Section 163 Code of Criminal Procedure: Duties of the Police
(1) The authorities and officials in the police force shall investigate criminal offences and shall take all measures that may not be deferred, in order to prevent concealment of facts. To this end they shall be entitled to request, and in exigent circumstances to demand, information from all authorities, as well as to conduct investigations of any kind insofar as there are no other statutory provisions specifically regulating their powers.
(2) The authorities and officials in the police force shall transmit their records to the public prosecution office without delay. Where it appears necessary that a judicial investigation be performed promptly, transmission directly to the Local Court shall be possible.
(3) Section 52 subsection (3), Section 55 subsection (2), Section 57 subsection (1) and Sections 58, 58a and 68 to 69 shall apply mutatis mutandis to the examination of a witness by officials in the police force. The decision on permission pursuant to Section 68 subsection (3), first sentence, and on the assignment of counsel to a witness shall be taken by the public prosecution office; in all other cases the necessary decisions shall be taken by the person in charge of the examination. Section 161a subsection (3), second to fourth sentences, shall apply mutatis mutandis to decisions by officials in the police force pursuant to Section 68b subsection (1), third sentence. Section 52 subsection (3) and Section 55 subsection (2) shall apply mutatis mutandis to the instruction of an expert by officials in the police force. In the cases referred to in Section 81c subsection (3), first and second sentences, Section 52 subsection (3) shall also apply mutatis mutandis to examinations by officials in the police force.
Section 95 Code of Criminal Procedure: Obligation to Surrender
(1) A person who has an object of the above-mentioned kind in his custody shall be obliged to produce it and to surrender it upon request.
(2) In the case of non-compliance, the regulatory and coercive measures set out in Section 70 may be used against such person. This shall not apply to persons who are entitled to refuse to testify.

Yes. Since the year 2004 cybercrime offences and offences committed by use of the internet are included as a special type of crimes in the Federal Police Agency's collection of data on crime. As those statistics only show detected crime (but not undetected cases or an indication of the dark figure), they are not very reliable to provide the true number of such offences.

(2) Is there in your country a website that provides data and information on the occurrence, seriousness, cost, impact etc. of cyber-crimes in your country? If "yes", provide the websites electronic address.

Yes:

Bundeslagebilder Cybercrime:

http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true

BSI-Lagebericht IT-Sicherheit:

https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html

A collection of links concerning statistics and information on cyber crime offences can be found at: http://www.cyber-crime.info/medien-material/internetdelinquenz/

(3) Do victimization surveys in your country include questions on cyber-crimes?

A regular and comprehensive survey on cyber crime is not available in Germany. Yet, several surveys that are not dedicated to cybercrime offences in particular nevertheless include some information thereto.

- Online-survey on security and delinquency on the internet 2006[198]
- Survey of the sexual victimization of girls and boys in chat-rooms[199]
- Surveys of the Federal Association for Information Technology, Telecommunications and New Media, BITKOM[200]
    - Confidence and security on the internet[201]
    - Protection of data on the internet[202]
    - Internet-security[203]

[198] http://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Kriminologisches_Seminar/Ergebnisse_SUDI_2006.pdf.
[199] *Katzer,* Die dunkle Seite der Chatkommunikation, http://emdr-innocenceendanger.org/fileadmin/PDFs-Deutsch/documents/Die_dunkle_Seite_der_Chatkommunikation_Maerz_2007.pdf.
[200] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
[201] http://www.bitkom.org/files/documents/Vertrauen_und_Sicherheit_im_Netz.pdf.
[202] http://www.bitkom.org/files/documents/BITKOM_Publikation_Datenschutz_im_Internet.pdf.
[203] http://www.bitkom.org/files/documents/BITKOM_Internet_Sicherheit_Extranet.pdf.

(4) What types of computer crime / computer fraud are most often reported in your country?

Offences committed by use of the internet as a whole: 222267 cases

- thereof Computer fraud: 167787 cases[204]

Cybercrime offences as a whole: 84.981 offences

- thereof computer fraud: 26.723 cases[205]
-

(5) Do law enforcement and prosecution in your country have a computer crimes unit? If so, how many officers/prosecutors are in it?

Yes; see for the Federal Police Agency „Zentralstelle für anlassunabhängige Recherchen in Datennetzen (ZaRD)“[206]

For the central police agencies of the German Länder:

Baden-Württemberg: Abt. 7 Cyberkriminalität / Digitale Spuren[207]

Bayern[208]

- Abteilung II Kriminaltechnische Institut, SG 210 Forensische IuK
- Abteilung VI Ermittlungen / Operative Spezialeinheiten, Dezernat 63 Operative Spezialeinheiten, SG 632 IT-Ermittlungsunterstützung/EASy, SG633 Kompetenzzentrum TKÜ-BY

Berlin

- LKA 3 - Abteilung für OK, Wirtschaftskriminalität & Betrug, Dezernat 33 u. 36[209]
- LKA 7 - Abteilung für Phänomenzentrierte Kriminalitätsbekämpfung, Ermittlungsunterstützung, Dienststelle LKA 72[210]

Brandenburg

- Abteilung LKA 100 „Zentralstellenaufgaben“: Einrichtung eines IuK-Kompetenzzentrums[211]
- Abteilung LKA 200 „Ermittlungen“: Zuteilung der Delikte der IuK-Kriminalität im engeren Sinne im Rahmen einer Neustrukturierung an das Dezernat „Wirtschaftskriminalität“

[204] *BKA,* PKS 2011, S. 261.
[205] *BKA,* PKS 2011, S. 254.
[206] http://www.bka.de/nn_204448/DE/DasBKA/Aufgaben/Zentralstellen/ZaRD/zard__node.html?__nnn=true.
[207] http://www.lka-bw.de/LKA/UeberUns/Documents/Organigramm_LKA.pdf.
[208] http://www.polizei.bayern.de/content/1/8/7/1/organigramm_internet.pdf.
[209] http://www.berlin.de/polizei/wir-ueber-uns/struktur/lka/lka3.html.
[210] http://www.berlin.de/polizei/wir-ueber-uns/struktur/lka/lka7.html.
[211] http://www.internetwache.brandenburg.de/sixcms/detail.php?id=252961&location=Organisation.

Bremen

- K 5 Wirtschafts- und Vermögenskriminalität, K 53 Allgemeiner Betrug, IuK-Kriminalität und Sonderdelikte Betrug[212]

Hessen

- Abteilung 3 - IuK-Einsatz und Cybercrime[213]

Niedersachen

- Abteilung 3 - Analyse, Prävention, Ermittlung, Dezernat 38 Zentralstelle Internetkriminalität

Nordrhein-Westfalen

- Abteilung 4 „IuK-Kriminalität, Ermittlungsunterstützung“

Rheinland-Pfalz[214]

- Abteilung 2 Einsatz- und Ermittlungsunterstützung, Dezernat 26 TKÜ Forensische IuK
- Abteilung 4 Auswertung und Ermittlungen, Dezernat 47 Cybercrime

Saarland

- Direktion LPP 2 Kriminalitätsbekämpfung/Landeskriminalamt, Abteilung LPP 22 Deliktsübergreifende Kriminalitätsbekämpfung, Dezernat LPP 222 Cybercrime (im Aufbau)[215]

Sachsen

- Abteilung 2 Ermittlung/Auswertung, Dezernat 25 Korruption/INES/IuK-Kriminalität[216]

Sachsen-Anhalt

- Abteilung 4 Auswertung, Analyse/Zentrale Ermittlungen/Prävention, Dezernat 42 Auswertung, Analyse/Wirtschaftskriminaltität/IuK-Kriminalität[217]

StA:

---

[212] http://www.polizei.bremen.de/sixcms/media.php/13/kripo.pdf.
[213] http://www.polizei.hessen.de/icc/internetzentral/nav/0cd/broker.jsp?uCon=f645085c-927b-99f3-362d-61611142c388&uBasVariant=11111111-1111-1111-1111-111111111111.
[214] http://www.polizei.rlp.de/internet/nav/72f/binarywriterservlet?imgUid=6c76840a-bdf6-8313-d587-31f42680e4cd&uBasVariant=22222222-2222-2222-2222-222222222222.
[215] http://www.saarland.de/dokumente/thema_polizei/LPP_Gesamt-Orga_20120301.pdf.
[216] http://www.polizei.sachsen.de/de/dokumente/LKA/aktuellXOrganigrammXLKA.pdf.
[217] http://www.sachsen-anhalt.de/fileadmin/Elementbibliothek/Bibliothek_Politik_und_Verwaltung/Bibliothek_TPA/lka/Presse/1007_Organigramm_LKA.PDF.

Baden-Württemberg

- Generalstaatsanwaltschaft Stuttgart, Abteilung I, Dezernat 17, Zentralstelle zur Bekämpfung der Kommunikations- und Informationskriminalität[218]
- Anzahl Mitarbeiter: 3

Brandenburg

- Staatsanwaltschaft Cottbus - Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer- und Datennetzkriminalität[219]

Hamburg

- Hauptabteilung VII (Sonderabteilungen), Abteilung 74, 14. Sonderdezernat: Computerstrafsachen[220]

Niedersachen

- Staatsanwaltschaft Göttingen - Schwerpunktstaatsanwaltschaft zur Bekämpfung der Kriminalität im Zusammenhang mit Informations- und Kommunikationstechnik[221]
- Staatsanwaltschaft Osnabrück - Abt. XII Internetkriminalität[222]
- Staatsanwaltschaft Verden – Abteilung VIII Zentralstelle für IuK-Kriminalität[223]

Nordrhein-Westfalen

- Staatsanwaltschaft Köln, Hauptabteilung C, Abteilung 119 Internet- und Computerkriminalität[224]

Thüringen

- Staatsanwaltschaft Mühlhausen, Schwerpunktabteilung zur Bekämpfung von Wirtschaftsstrafsachen und IT-Kriminalität[225]

(6) Does your or any law school in the country offer courses on cyber-crime? Please provide a website address.

Yes, such courses can be found at the following universities:

University of Bonn:

[218] http://www.generalstaatsanwaltschaft-stuttgart.de/servlet/PB/show/1208979/Organigramm01.07.07.pdf.
[219] http://www.sta-cottbus.brandenburg.de/sixcms/detail.php?gsid=bb2.c.541158.de&template=seite_stcb_aufg.
[220] http://justiz.hamburg.de/contentblob/1423764/data/hauptabteilung-vii.pdf.
[221] http://www.staatsanwaltschaften.niedersachsen.de/portal/live.php?navigation_id=22921&article_id=81208&_psmand=165.
[222] http://www.staatsanwaltschaften.niedersachsen.de/portal/live.php?navigation_id=22942&article_id=81570&_psmand=165.
[223] http://www.staatsanwaltschaften.niedersachsen.de/portal/live.php?navigation_id=22950&article_id=81207&_psmand=165.
[224] http://www.sta-koeln.nrw.de/wir/15_organisation/index.php.
[225] http://www.thueringen.de/de/thgsta/staatsanwaltschaften/sta_muehlhausen/.

- Lecture on „Internetdelinquenz“
- http://www.jura.uni-bonn.de/index.php?id=1512

University of Frankfurt/Oder:

- Lecture on „media criminal law“
- http://www.rewi.europa-uni.de/de/studium/Deutsch/SBP/anlage2_ab1_10_2010.html

University of Freiburg:

- Lecture on „Criminal law on information“
- http://www.jura.uni-freiburg.de/studium/pruefungsamt/SPB-Studium/studienplan/studienplan-stand-01.04.2012-nur-spb-studium
- http://www.jura.uni-freiburg.de/studium/pruefungsamt/SPB-Studium/SPB-Infoheft/view

Bucerius Law School Hamburg:

- Lecture on Computer and Multimedia Criminal Law
- http://www.law-school.de/fileadmin/user_upload/medien/BLS-Publikationen/ZwiSchwerPO_Juli_2008.pdf

University of Cologne:

- Lecture on media criminal law
- https://klips.uni-ko-eln.de/qisserver/rds?state=verpublish&status=init&vmfile=no&publishid=125046&moduleCall=webInfo&publishConfFile=webInfo&publishSubDir=veranstaltung

University of Leipzig:

- Lecture on Media criminal law
- http://www.uni-leipzig.de/~jura/index.php/studium/studienwechsler/schwerpunktbereiche/33-schwerpunktbereich-qmedien-und-informationsrechtq-v15-33.html

University of Mainz:

- LL.M. programme on media law
- http://www.mainzer-medieninstitut.de/studiengang/inhalte-und-ablauf.php

University of Potsdam:

- Lectures on media criminal law
- http://www.uni-potsdam.de/ambek/ambek2010/13/Seite3.pdf

University of Saarland:

- Lectures on media criminal law

- http://www.uni-saar-land.de/fileadmin/user_upload/Campus/Service/Recht_und_Datenschutz/Recht_der_Universitaet/Ausbildungs-_Pruefungs-_Studienordnungen/DB09-496.pdf

University of Würzburg:

- Criminal law on media and computer
- http://www.jura.uni-wuerzburg.de/studium/studium_der_rechtswissenschaft_erste_juristische_pruefung/schwerpunktbereichsstudium/s_5_kriminalwissenschaften/

(7) Is the subject of cybercrime included in the training and/or continuing education of judges, prosecutors and police?

See for the education of judges and prosecutors (6).

For the education of police officers see for example the programmes of

Bayern:

- Education on information technology and police IT-knowledge[226]

Hamburg:

- Cybercrime offences[227]

Hessen:

- Information technology[228]

Mecklenburg-Vorpommern:

- Computer and Internet Crime[229]

(8) Please identify whether the following forms and means of cybercrime (1) occur frequently, (2) occur infrequently, or (3) have not occurred in your country, by placing an "X" as appropriate in the following table:

Forms and Means of Cyber-Crime	Occur Frequently	Occur Infrequently	Has not Occurred
Online identity theft (including phishing and online trafficking in false identity information)	X		

[226] http://www.polizei.bayern.de/wir/aufgaben/index.html/1688.
[227] http://hdp.hamburg.de/contentblob/2283696/data/moduluebersicht-polizei.pdf.
[228] http://www.hfpv.hessen.de/irj/VFH_Internet?cid=fa35ec2d774c7d685f06fc61040000e3.
[229] http://www.polizei.mvnet.de/cms2/Polizei_prod/Polizei/de/bi/Ausbildungsstufen/Laufbahngruppe_2%2c_1._Einstiegsamt__%28ehemals_gehobener_Dienst%29/index.jsp.

Hacking (illegal intrusion into computer systems; theft of information from computer systems)	X		
Malicious code (worms, viruses, malware and spyware)	x		
Illegal interception of computer data		x	
Online commission of intellectual property crimes		x	
Online trafficking in child pornography		x	
Intentional damage to computer systems or data		x	
Others[230]			

(9) In addition, to the above, if there are any other forms and means of cyber-crime that have occurred (either frequently or infrequently) in your country, please identify them as well as the frequency with which the occur in the following table:

See (D)(8) and:

Forms and Means of Conduct	Occur Frequently	Occur Infrequently
Fraud	x	
Computer fraud	X	
Forgery of data intended to provide proof, Meaning of deception in the context of data procession	X	

[230] See (D)(9).